

FILED UNDER SEAL

BATHAE DUNNE LLP

Yavar Bathae (CA 282388)
yavar@bathaeedunne.com
Edward M. Grauman (*pro hac vice*)
egrauman@bathaeedunne.com
Andrew C. Wolinsky
awolinsky@bathaeedunne.com
445 Park Avenue, 9th Floor
New York, NY 10022
Tel.: (332) 322-8835

Brian J. Dunne (CA 275689)
bdunne@bathaeedunne.com
633 West Fifth Street, 26th Floor
Los Angeles, CA 90071
Tel.: (213) 462-2772

*Interim Co-Lead Counsel for the
Advertiser Class*

SCOTT + SCOTT ATTORNEYS AT LAW LLP

Kristen M. Anderson (CA 246108)
kanderson@scott-scott.com
230 Park Avenue, 17th Floor
New York, NY 10169
Tel.: (212) 223-6444

Christopher M. Burke (CA 214799)
cburke@scott-scott.com
David H. Goldberger (CA 225869)
dgoldberger@scott-scott.com
Kate Lv (CA 302704)
klv@scott-scott.com
600 W. Broadway, Suite 3300
San Diego, CA 92101
Tel.: (619) 233-4565

Patrick J. McGahan (*pro hac vice*)
pmcgahan@scott-scott.com
Michael P. Srodoski (*pro hac vice*)
msrodoski@scott-scott.com
156 South Main Street, P.O. Box 192
Colchester, CT 06415
Tel.: (860) 537-5537

(Additional counsel on signature page)

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MAXIMILIAN KLEIN, et al., on behalf of themselves
and all others similarly situated,

Plaintiffs,

v.

META PLATFORMS, INC.,

Defendant.

Case No. 20-cv-08570-JD

The Hon. James Donato

**FIRST AMENDED CONSOLIDATED
ADVERTISER CLASS ACTION
COMPLAINT**

DEMAND FOR JURY TRIAL

CLASS ACTION

FILED UNDER SEAL**TABLE OF CONTENTS**

1		
2	INTRODUCTION	1
3	PARTIES	5
4	I. PLAINTIFFS	5
5	II. DEFENDANT	6
6	JURISDICTION AND VENUE	8
7	INTRADISTRICT ASSIGNMENT	9
8	FACTS.....	9
9	I. FACEBOOK EMERGES AS THE DOMINANT SOCIAL NETWORK.....	9
10	A. The Last Social Network Standing.....	9
11	B. A New Market of Its Own Creation	11
12	C. The Data Targeting Barrier to Entry.....	13
13	D. Google’s Failed Entry into the Social Advertising Market	16
14	II. A THREAT TO FACEBOOK’S MONOPOLY: THE RISE OF SMARTPHONES AND	
15	MOBILE APPS	19
16	A. The Mobile App Revolution.....	19
17	B. Facebook Recognizes the Looming Threat Presented by Mobile Applications.....	22
18	C. The Facebook Platform	23
19	D. The Profitable Open Graph Platform and Mobile Install Business	26
20	III. FACEBOOK WEAPONIZES ITS PLATFORM TO DESTROY COMPETITION.....	28
21	A. Facebook Makes Plans to Remove Vital Platform Functionality and Refuses to Sell	
22	Social Data to Competing Application Developers.....	28
23	B. Facebook’s Social Data Heist.....	31
24	C. Facebook Targets Its Competitors for Reciprocity or Denial of API Access	35
25	D. Facebook Decides to Add the Events API to Its Reciprocity Scheme	39
26	E. The Decision to Remove Developer Access to the Friends, News Feed, Events, and	
27	Other Crucial APIs Lacked Any Legitimate Justification.....	41
28	F. Facebook Prepares to Announce Removal of the APIs.....	45
	G. The Announcement at F8	49
	IV. THE SURVEILLANCE AND ACQUISITION OF COMPETITIVE THREATS	50
	A. Facebook Relies on Onavo’s Surveillance of Facebook’s Competitors, and Acquires	
	and Uses Onavo’s Assets.....	51
	B. Facebook Identifies Instagram as a Threat and Acquires the Company	55

FILED UNDER SEAL

1	C. Facebook Acquires WhatsApp	63
2	V. FACEBOOK CONTINUES TO ENTER INTO EXTENDED API AGREEMENTS AFTER	
3	THE APRIL 2015 PLATFORM CHANGES.....	69
4	A. Facebook Continues to Enter Into Whitelist Agreements for Events API	
5	Functionality.....	69
6	B. Facebook Continues to Enter Into Whitelist Agreements for Friends API	
7	Functionality.....	71
8	VI. FACEBOOK’S NEED FOR “SIGNAL” FROM WITHIN ITS WALLED GARDEN AND ITS	
9	EXPANSION INTO NEW SOURCES OF SOCIAL DATA.	72
10	A. The Aftermath of the Platform Change and the App Vacuum.	72
11	B. Facebook Relies on User Identity and Engagement to Derive Critical User Intent	
12	Data.....	73
13	C. Facebook Ventures into E-Commerce to Obtain Signals.....	75
14	D. Facebook Moves into Location-Based Services.....	84
15	E. Streaming Video and Facebook Watch	88
16	VII. FACEBOOK’S ENTRY AND DATA CAPTURE CONDUCT	92
17	A. Facebook Enters Markets to Leverage Agreements that Maintain and Fortify Its	
18	Social Advertising Monopoly.....	92
19	B. Facebook Enters into an Anticompetitive Data Agreement with Foursquare	97
20	C. Facebook Enters into an Agreement with eBay to Preserve Its Social Advertising	
21	Monopoly and to Strengthen the Data Targeting Barrier to Entry	100
22	1. Facebook’s Announcement of Marketplace Causes Concern for eBay, and eBay	
23	Threatens to Pull Ad Revenue Unless Facebook Siloed Data from eBay Ads. ...	100
24	2. The Facebook and eBay Agreement Not to Compete with Each Other	110
25	3. Facebook’s Agreement with eBay Impaired Its Marketplace Product and	
26	Strengthened Its Core Ad Business	112
27	D. Facebook Enters into an Anticompetitive Data Sharing Agreement with Netflix	113
28	1. Reed Hastings and the Facebook-Netflix Relationship.....	113
	2. Facebook’s Entry at Scale Threatens Competition with Netflix	119
	3. Facebook and Netflix Enter into Amended Agreements.....	121
	4. Facebook and Netflix Agree Not to Compete in Each Other’s Market.....	125
	VIII. FACEBOOK ANTICOMPETITIVELY USED ONAVO DATA TO BUILD A MASSIVE,	
	MACHINE-LEARNING-DRIVEN SURVEILLANCE SYSTEM AND TO SPY ON	
	FACEBOOK USERS EVEN WHEN USING NON-FACEBOOK APPS.	130
	A. Onavo’s Spyware Secretly Shuttles Sensitive User Data to Facebook for Its Internal	
	Machine Learning Models.....	131

FILED UNDER SEAL

1	B.	Facebook Used Stolen Onavo Data Together with User Data from Its Own Apps to Build a Granular and Real-time Competitive Surveillance System.	135
2	C.	Facebook Matched the Onavo Data It Collected from Users on Other Apps with their Facebook IDs and Stored User Data in Its “Hive” Database.	136
3	IX.	THE THREAT BEYOND FACEBOOK’S WALLED GARDEN	138
4	A.	Facebook Audience Network	138
5	B.	Facebook Acquires Atlas.....	140
6	C.	Facebook Positions Itself Against Google by Combining Atlas, Audience Network, and Other Technology	144
7	D.	Shadow Profiles and Identifying Users Outside of Facebook’s Apps.....	146
8	X.	FACEBOOK AND GOOGLE AGREE NOT TO COMPETE AND TO FORTIFY THE FACEBOOK-DOMINATED SOCIAL ADVERTISING MARKET	147
9	A.	Google’s Dominance Over Ad Exchanges and Ad Servers and the Looming Facebook Threat.....	147
10	B.	Google’s AI Dominance	149
11	C.	The Rise of Header Bidding and Facebook’s Threat to Compete with Google	151
12	D.	Google Agrees to Help Facebook Identify Facebook’s Own Users Outside of Its Walled Garden, and Facebook Backs Off of Programmatic and Exchange-Trade Advertising	153
13	XI.	FACEBOOK ANTICOMPETITIVELY INTEGRATES THE BACKENDS OF INSTAGRAM, WHATSAPP, MESSENGER, AND ITS CORE FACEBOOK PRODUCT	155
14	A.	Facebook’s Social Data Refinement, Signal Extraction, Data Structuring, and Feature Creation Process.	156
15	B.	Facebook and Identity	163
16	C.	Facebook Begins a Rapid Back-End Integration Effort in Response to Antitrust Scrutiny.....	165
17	D.	The Call to Break Up Facebook, WhatsApp, and Instagram	167
18	E.	Zuckerberg Decides to Integrate Facebook, Instagram, and WhatsApp, and Plans a Pretextual Smokescreen to Avoid Backlash from Antitrust Regulators.....	168
19	F.	Facebook Anticompetitively Integrates Its Products’ Back Ends, Creating Unified Data Stores and AI/ML Systems	173
20	1.	Facebook Forces Its Products to Use Features Instead of Signals and Raw Social Data to Build AI and ML Models, Making the Company’s Social Data Impossible Disaggregate by Source or Line of Business.....	174
21	2.	Facebook Centralizes AI and ML Model Architectures and Testing.....	177
22	G.	Zuckerberg’s End-to-End Encryption Smokescreen Was Pretextual and Lacked a Legitimate Technical Justification.....	178
23			
24			
25			
26			
27			
28			

FILED UNDER SEAL

1	XII. THE RELEVANT MARKET	181
2	A. The Social Advertising Market.....	181
3	B. Barriers to Entry	188
4	C. Relevant Geographic Market.....	190
5	XIII. HARM TO COMPETITION AND ANTITRUST INJURY	191
6	CLASS ACTION ALLEGATIONS	195
7	CLAIMS FOR RELIEF	201
8	PRAYER FOR RELIEF	204
9	JURY DEMAND.....	205

FILED UNDER SEAL**INTRODUCTION**

1
2 1. This Complaint is brought on behalf of people and companies—including each of the
3 named Plaintiffs—who bought advertising from Defendant Meta Platforms, Inc.¹ (“Facebook”) at
4 anticompetitively inflated prices. Over the course of the past decade, Facebook devised, executed, and
5 reaped the benefits of a scheme to unlawfully monopolize the market for social advertising. As a direct
6 result, Facebook was able to (and in fact, did) charge supracompetitive prices for social advertisements
7 to thousands of people and businesses, including Plaintiffs Affilious, Inc., Jessyca Frederick, Mark
8 Young, Joshua Jeon, 406 Property Services, PLLC, Mark Berney, and Katherine Looper.

9 2. Facebook acquired the power to raise prices through the anticompetitive scheme described
10 below and did so year after year with no competitive check.

11 * * *

12 3. By the end of 2010, Facebook had emerged the victor among social networks and had
13 begun monetizing its product through targeted advertising. Facebook had obtained a monopoly in a form
14 of online advertising that was distinct from others—social advertising. This form of advertising relied on
15 a particular form of data, called social data, to power machine learning and AI models used for advertising
16 and content targeting.

17 4. Facebook had acquired a critical mass of social data and targeting infrastructure, giving
18 rise to a Data Targeting Barrier to Entry (“DTBE”)—a network-driven barrier to entry that protected
19 Facebook’s monopoly share of the Social Advertising Market.

20 5. Facebook’s dominance was threatened in 2012, and to fend off this threat Facebook’s CEO
21 Mark Zuckerberg and his senior lieutenants planned and executed a scheme between 2012 and 2015 that
22 leveraged Facebook’s developer Platform to extract social data and advertising revenue from third-party
23 apps, some of which posed a competitive threat to Facebook. During this period, Facebook overtly
24 destroyed its actual and potential competition, and acquired two then-nascent threats to its business,
25 Instagram and WhatsApp.

26
27 ¹ Originally-named Defendant Facebook, Inc. changed its name to Meta Platforms, Inc., during
28 the pendency of this case.

FILED UNDER SEAL

1 6. By April 2015, Facebook had expelled third-party apps from its Platform, including by
2 purporting to deprecate core functionality such as traversing a user's Facebook friends, news feed, or
3 Events functionality. Before this move, Facebook had been able to harvest social data from apps built on
4 its Platform. Afterwards, however, Facebook faced a social data vacuum. Facebook entered into a series
5 of data sharing and whitelist agreements to obtain vital data and advertising revenue, including throughout
6 2017, 2018, and the first half of 2019.

7 7. Yet Facebook was still in need of what it called "signals"—refined social data that could
8 be used as part of its AI and ML models. To obtain those signals, Facebook needed access to data
9 harvested by what Facebook internally referred to as "sub-vertical" apps, such as video, location, and e-
10 commerce apps. Data from these apps was close to the point of conversion (*i.e.*, customer sales) and was
11 closely guarded by leaders in each sub-vertical.

12 8. To obtain data from these companies, from 2016 to 2018 Facebook entered targeted sub-
13 verticals, threatening ruinous competition and then withdrawing in exchange for an agreement by a leader
14 in that sub-vertical to hand over signal-rich social data to Facebook, strengthening its dominant position
15 in the Social Advertising Market and the DTBE.

16 9. Thus, Facebook entered the streaming video business with a product called Watch,
17 extracted data (and several hundred million dollars in advertising commitments) from the then-leader,
18 Netflix—whose CEO sat on Facebook's board—then systematically withdrew from the business,
19 hindering the data-driven brains behind its new video product and scuttling its investment in original
20 content.

21 10. Facebook executed the same maneuver with eBay, developing a Facebook Marketplace
22 product, then crippling it in exchange for social data and ad purchases from the e-commerce giant.

23 11. Facebook also entered into an agreement with its direct competitor, Foursquare, to capture
24 location data that Foursquare had painstakingly collected from its users. Facebook extracted this deal
25 after having entered the location-based social networking business, putting pressure on Foursquare to
26 capitulate.

FILED UNDER SEAL

12. Facebook also expanded its Onavo spyware apparatus—which it had used from 2011 to 2015 as part of its Platform scheme—to subvert competition in the years thereafter.

13. From 2016 through 2019, Facebook expanded its collection of user data from smartphones and devices around the world by offering spyware—sham VPN programs and app-locking programs that secretly captured Internet traffic from mobile devices, including messaging, battery, and third-party app usage information, then relayed this information to Facebook for use in its internal models.

14. Facebook paired the data it stole from users using Onavo with its newly acquired Instagram and WhatsApp properties in order to validate its AI and ML models, which in turn provided Facebook with a real-time view of all of its competitors. Facebook also matched users it surveilled with internal Facebook IDs, allowing Facebook to obtain granular demographic and targeting information and AI/ML-derived inferences for its business. Put simply, Facebook used stolen user data, deceptively obtained through spyware, to spy on users as they interacted with non-Facebook apps, such as Snapchat and YouTube. Using that same user data, Facebook built the largest real-time surveillance system to ever exist—an infrastructure unavailable to any of Facebook’s competitors.

15. As the 2010s wore on, technological developments in header bidding and Google’s acquisition and deployment of powerful machine learning tools across its growing data collection ecosystem threatened to erode Facebook’s identity-based targeting advantage—and perhaps even superset the Social Advertising Market. Facebook responded by acquiring and expanding powerful cross-site and cross-device tracking tools, deploying its own machine learning tools outside its walled garden, and laying the groundwork to enter programmatic advertising and other Google-dominated online ad markets. By 2018, the two online advertising titans—each with its own long-running sphere of dominance—were headed for a direct clash.

16. Except that instead of competing, Facebook and Google actually cut an anticompetitive deal. Codenamed “Jedi Blue,” this September 2018 agreement between Facebook and Google divided markets between the two companies and not only reinforced but bolstered Facebook’s dominant position in the Social Advertising Market.

FILED UNDER SEAL

1 17. Pursuant to the Jedi Blue agreement, Facebook dropped its support for header bidding,
2 effectively ceding the programmatic and exchange-based ad markets to Google. At the same time, Google
3 agreed to provide Facebook powerful tools to identify, target, and monetize Facebook’s own users on the
4 web and across third-party mobile applications, then give Facebook priority over 90% of advertisements
5 to these users and twice the amount of time to bid on advertising to them.

6 18. The net effect was that Facebook remained the dominant—and only—source of granularly
7 targeted advertising to its social-networking user base. In exchange, Facebook backed away from
8 Google’s advertising exchange business, including by forgoing the adoption of “header bidding.”

9 19. As a result of the conduct set forth above, Facebook became and remained for nearly a
10 decade the dominant (and in many respects, sole) source for highly valuable advertising that could
11 precisely target networks of users in a social network. Facebook has used this market power to repeatedly
12 raise advertising prices every year since it began its scheme.

13 20. Finally, with Google watching Facebook’s flank, Facebook turned to fortifying its Social
14 Advertising monopoly, particularly from regulators. As calls to break up and/or regulate Facebook
15 strengthened, Facebook rushed to force its organization to adopt a common “feature” framework, called
16 the Facebook Feature Framework, for its AI/ML systems, reducing the flexibility of the systems yet
17 inextricably intertwining the data obtained from Facebook’s properties. Facebook also forced its
18 organization to adopt pre-trained ML models, further reducing the flexibility of each of its business units
19 to devise AI and ML suited for their particular tasks.

20 21. Internally, Mark Zuckerberg and his highest-level PR executives devised a smokescreen
21 to mask the above integration conduct from regulators: end-to-end encryption. Whether or not Facebook
22 encrypted its apps, however, had nothing to do with the integration—and indeed, Facebook had already
23 implemented end-to-end encryption years prior in its WhatsApp product. Nonetheless, Facebook took to
24 the press with its carefully-planned pretext, claiming that the company’s massive integration of the
25 backend of its products was about end-to-end encryption (it was not), rather than an attempt to prevent
26 regulators from effectively divesting or otherwise disaggregating Facebook’s products and data.

FILED UNDER SEAL

22. Over the course of nearly a decade, Facebook has faced no meaningful competitive check on social advertising prices—and it has extracted supracompetitive revenues from advertisers like Plaintiffs throughout this period.

23. Plaintiffs are advertisers on Facebook’s advertising platform that were injured by paying supracompetitive prices for social advertising. The prices they paid would have been lower if Facebook had not unlawfully monopolized the Social Advertising Market and taken unlawful acts (including an express anticompetitive agreement with Google) to maintain that monopoly, as those prices would have been subject to competitive forces that would otherwise exist as a check on Facebook’s market power and monopoly.

PARTIES**I. PLAINTIFFS**

24. Plaintiff Affilious, Inc. (“Affilious”) is a California corporation with its principal place of business in La Quinta, California. Affilious is an internet publisher firm that operates several websites, including WineClubReviews.net. In late 2016 and in August 2017, Affilious purchased advertising on Facebook’s self-service advertising platform to promote WineClubReviews.net. Until no earlier than November 6, 2019, Affilious did not know, and could not reasonably have known, the truth about Facebook’s anticompetitive conduct, including its purpose and intent to engage in anticompetitive conduct, nor could it have known that it had been injured by paying supracompetitive prices for advertising.

25. Plaintiff Jessyca Frederick is a citizen of the State of California. Frederick was the sole proprietor of ClubsAndGifts.com, a promotional website, and a founder and CEO of Affilious. At various times from April 4, 2009, through August 2017, Frederick purchased advertising on Facebook’s self-service advertising platform to promote her businesses.

26. Plaintiff Mark Young is a citizen of the State of New York. Young is the sole proprietor of Dinkum Hair, a hair salon located in Buchanan, New York. Young d/b/a Dinkum Hair purchased advertising on Facebook’s self-service advertising platform to promote the business between June 2017 and April 2019.

FILED UNDER SEAL

27. Plaintiff Joshua Jeon is a citizen of the State of Texas. He is a pastor at Dwell Church in Austin, Texas. In April 2016, Jeon purchased advertising on Facebook’s self-service advertising platform to promote Dwell Church. Jeon did not receive reimbursement from Dwell Church for the purchase.

28. Plaintiff 406 Property Services, PLLC (“406 Property Services”) is a Montana professional limited liability company with its principal place of business in Whitefish, Montana. 406 Property Services is a real estate property services company. From approximately June 8, 2017, until approximately October 20, 2017, 406 Property Services purchased advertising on Facebook’s self-service advertising platform to promote its business.

29. Plaintiff Mark Berney is a citizen of the State of Montana. From in or about 2016 into December 2018, Berney purchased advertising on Facebook’s self-service advertising platform to promote his personal musical work.

30. Plaintiff Katherine Looper is a citizen of the State of California. From in or about 2013 through March 2020, Looper purchased advertising on Facebook’s self-service advertising platform to promote free musical concerts at the Cadillac Hotel, a residential hotel for low-income persons in San Francisco operated by Looper’s nonprofit organization, Reality House West.

31. Plaintiffs all paid prices for advertising that were higher than they would have been absent Facebook’s anticompetitive conduct and unlawfully acquired and/or maintained monopoly. Facebook caused Plaintiffs to pay supracompetitive prices for advertising as a result of the market power it obtained and/or maintained as a result of the anticompetitive scheme described in this Complaint.

II. DEFENDANT

32. Defendant Meta Platforms, Inc., is a publicly traded company, incorporated in Delaware. Meta Platforms, Inc. was formerly known as Facebook, Inc., and changed its name to Meta Platforms, Inc. on October 28, 2021. Facebook’s principal place of business and headquarters is located at 1601 Willow Road in Menlo Park, California.

33. Founded in 2004 by Mark Zuckerberg, Facebook is a social media company that provides online services to billions of users around the world. In exchange for providing services, Facebook

FILED UNDER SEAL

collects user data, which it uses to create and sell targeted advertising services. Facebook's principal revenue is from targeted social media advertising that it provides to advertisers as a data broker.

34. Facebook also operates as a platform for third-party applications and hardware, and owns and operates several business divisions:

- Facebook. Facebook's core application, which bears the company's name, is, according to Facebook's filing with shareholders, designed to enable "people to connect, share, discover, and communicate with each other on mobile devices and personal computers." The Facebook core product contains a "News Feed" that displays an algorithmically ranked series of stories and advertisements individualized for each person.
- Instagram. Instagram is a photo-sharing application that allows users to share photos, videos, and messages on mobile devices. Instagram was acquired in April 2012, and at present, Facebook operates Instagram as a separate application from its core Facebook product.
- Messenger. Facebook's Messenger application is a multimedia messaging application, allowing messages that include photos and videos to be sent from person to person across platforms and devices.
- WhatsApp. WhatsApp is a secure messaging application used by individuals and businesses. WhatsApp was acquired by Facebook in 2014 for \$21.8 billion, and at the time had approximately 450 million users worldwide.
- Oculus. Oculus is Facebook's virtual reality hardware line of business, which Facebook acquired in March 2014 for approximately \$2 billion.

35. Facebook's revenue as of year-end 2019 was \$70.70 billion (up 27% from the previous year), with net income from operations of \$23.99 billion. Almost all of this revenue came from advertising, particularly mobile advertising. As of year-end 2019, Facebook maintained \$54.86 billion in cash and cash-equivalent securities. Facebook employed 44,942 people around the world at the end of 2019 (up 26% from the previous year). Facebook's revenue as of year-end 2020 was \$85.97 billion (a 22% increase from the previous year), with net income from operations of \$32.67 billion. Again, almost

FILED UNDER SEAL

1 all of that revenue came from mobile advertising. As of year-end 2020, Facebook maintained \$61.95
2 billion in cash and cash-equivalent securities. Facebook employed 58,604 people around the world at the
3 end of 2020 (up 30% from the previous year). In 2021, Facebook / Meta earned \$117.93 billion in
4 revenue, of which \$114.93 billion came from advertising. The company's 2021 total income from
5 operations was \$46.753 billion. Disregarding Facebook / Meta's Reality Labs division (which operated
6 at a substantial loss), Facebook / Meta's total income from operations in 2021 was \$56.95 billion.
7 Facebook / Meta's net income from operations (including Reality Labs) in 2021 was \$39.37 billion

8 36. For the 2019 fiscal year, Facebook reported to investors that on average it had 1.66 billion
9 daily active users of Facebook and Messenger ("DAUs") (up 9% from the previous year) and 2.50 billion
10 monthly active users ("MAUs") (up 8% from the previous year). Facebook also reported that on average
11 it had 2.26 billion daily active people ("DAP") who used any Facebook product (up 11% from the
12 previous year) and 2.89 billion monthly active people ("MAP") (up 9% from the previous year). For the
13 2020 fiscal year, Facebook reported to investors that on average it had 1.84 billion DAUs (up 11% from
14 the previous year) and 2.80 billion MAUs (up 12% from the previous year). Facebook also reported that
15 on average it had 2.60 billion DAP who used any Facebook product (up 15% from the previous year).
16 For the 2021 fiscal year, Facebook / Meta reported to investors that on average it had 1.91 billion DAUs,
17 2.89 billion MAUs, 2.78 billion DAP, and 3.53 billion MAP, across its family of products—an increase
18 from 2020 in all four categories.

JURISDICTION AND VENUE

19
20 37. This action arises under Sections 1 and 2 of the Sherman Antitrust Act (15 U.S.C. §§ 1,
21 2) and Sections 4 and 16 of the Clayton Act (15 U.S.C. §§ 15, 26). The action seeks to recover treble
22 damages, interest, costs of suit, equitable relief, and reasonable attorneys' fees for damages to Plaintiffs
23 and members of the Classes resulting from Defendant's restraints of trade and monopolization of the
24 Social Advertising Market described herein.

25 38. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 (federal question),
26 1332 (class action diversity jurisdiction), and 1337(a) (antitrust); and under 15 U.S.C. § 15 (antitrust).

FILED UNDER SEAL

39. Venue is appropriate in this district under 15 U.S.C. § 15(a) (Clayton Act), 15 U.S.C. § 22 (nationwide venue for antitrust matters), and 28 U.S.C. § 1391(b) (general venue provision). Facebook transacts business within this district, and it transacts its affairs and carries out interstate trade and commerce, in substantial part, in this district.

40. The Court has personal jurisdiction over Facebook as it is subject to general jurisdiction in the State of California, where it maintains its headquarters and its principal place of business. The scheme, conspiracy, and monopolization alleged in this Complaint was targeted at individuals throughout the United States, causing injury to persons in the United States, including in this district.

INTRADISTRICT ASSIGNMENT

41. This action has been assigned to the Hon. James Donato of the San Francisco Division of this judicial district.

FACTS**I. FACEBOOK EMERGES AS THE DOMINANT SOCIAL NETWORK****A. The Last Social Network Standing**

42. Facebook's meteoric rise since its founding in 2004 is well documented. The company—started in the dorm room of its CEO Mark Zuckerberg as “the facebook”—rose to prominence in the face of fierce competition from several social networks. Initially an exclusive service for elite universities throughout the United States, Facebook eventually expanded its network to encompass a general audience of users throughout the United States and worldwide.

43. Between 2004 and 2010, Facebook vanquished a number of rivals, emerging as the dominant social network in the United States.

44. Facebook's first chief competitor was MySpace. Founded in 2003 (a year before Facebook), MySpace targeted the same audience, provided largely the same services, and rapidly attracted an enormous number of users. By 2005, MySpace had 25 million active users, and was acquired by NewsCorp for \$580 million. In 2006, MySpace registered 100 million users, passing Google as the most visited website in the United States.

FILED UNDER SEAL

1 45. However, the next three years featured a steady downward spiral for MySpace—and
2 countervailing growth by Facebook. In 2008, Facebook passed MySpace in worldwide active users and
3 continued to grow, reaching 307 million active users across the globe by April 2009. In May 2009,
4 Facebook passed MySpace in United States, 70.28 million to 70.26 million monthly active users.

5 46. MySpace never came close to Facebook again. By 2010, MySpace had mostly exited the
6 market, leaving the business of social media for good. MySpace’s CEO capitulated in November of 2010:
7 “MySpace is not a social network anymore. It is now a social entertainment destination.” In September
8 2010, MySpace reported that it had lost \$126 million, and in June 2011, NewsCorp sold the company for
9 \$35 million—\$545 million less than it had paid just six years earlier. By then, its user base had dwindled
10 to just 3 million monthly visitors.

11 47. During the same time period, several other social networks also met their demise,
12 including Google’s Orkut, AOL’s Bebo, and Friendster, which failed to scale rapidly enough to compete
13 with MySpace and Facebook.

14 48. By 2009 and through 2010, Facebook emerged as the only peer-to-peer social media
15 network to exist at scale, and no other network or company rivaled Facebook’s massive user base. On
16 March 2, 2010, *Adweek* reported that Facebook had booked revenues of up to \$700 million in 2009 and
17 was on track for \$1.1 billion in 2010—almost all from advertising to its newly won users. Facebook had
18 been roughly doubling its revenues every year up until that point—\$150 million in 2007, \$280-300
19 million in 2008, and \$700 million in 2009.

FILED UNDER SEAL

49. *Time* magazine heralded Zuckerberg as its 2010 Person of the Year.



50. *Time*'s cover story set out the stakes—the scope of the newly assembled social network was unprecedented and staggering:

What just happened? In less than seven years, Zuckerberg wired together a twelfth of humanity into a single network, thereby creating a social entity almost twice as large as the U.S. If Facebook were a country it would be the third largest, behind only China and India. It started out as a lark, a diversion, but it has turned into something real, something that has changed the way human beings relate to one another on a species-wide scale. We are now running our social lives through a for-profit network that, on paper at least, has made Zuckerberg a billionaire six times over.

51. By 2010, Facebook was unrivaled and dominant in a way no company since Microsoft had been in post-personal-computer history. And it had done so by riding the currents of powerful network effects.

B. A New Market of Its Own Creation

52. By the beginning of the millennium's second decade, Facebook was the indisputable king of an entirely new market—a market built not on hardware or operating system dominance, but one built on a network of people, with its power and value directly derived from their engagement with that

FILED UNDER SEAL

1 network. The more data users fed into Facebook by communicating and interacting with each other,
2 posting their pictures, and publishing their content, the more valuable the Facebook network became to
3 third parties, who could advertise to Facebook's users by targeting them using the very information they
4 provided to Facebook's network.

5 53. Data about what information users shared on their personal pages; the photos and profiles
6 they viewed; their connections to others; what they shared with others; and even what they put in
7 messages to other users all allowed targeted advertising on a scale that had never before existed. Unlike
8 search advertising, Facebook's advertising platform allowed advertisers to target Facebook's user base
9 by their attributes and behavior, not by a query entered into a search box. More importantly, unlike in
10 search, user identity was not only discoverable, it was willingly provided by users—as was the identity
11 of those users' closest friends and family members. These identities could be tracked and targeted
12 throughout the Internet.

13 54. This social data created by Facebook's network of engaged users could be monetized in a
14 number of ways. The data could be resold for targeted advertising and machine learning; Facebook's
15 machine learning algorithms mined patterns in the data for advertisers, which allowed advertisers to reach
16 precisely the right audience to convert into sales, user sign-ups, or the generation of sales leads. The data
17 also could be sold by commercializing access—for example, by providing application developers, content
18 generators, and advertisers with direct access to the information embedded in Facebook's network, such
19 as the interconnection between users, user attributes, and user behavior. That data then could be mined
20 by these third parties.

21 55. All the methods of monetizing social data were based on selling that data, but such data
22 could be packaged, structured, or mined differently depending on the application for which it was being
23 sold. For advertisers, Facebook's network presented advertisers and Facebook itself with entirely new
24 social signals, such as relationships, events, friendships, and granular interests. Movies, music, and books
25 were inherent parts of a user's profile. The amount of information in Facebook's network that could be
26 mined as social data was unprecedented—and Facebook received all that data daily from its millions of
27 users in the United States and worldwide.
28

FILED UNDER SEAL

1 56. The data Facebook collected was uniquely social, derived from the engaged interactions
2 and strong identity of Facebook’s users. Twitter, a public-facing social network, loosely enforced identity
3 and never required users to disclose granular details about themselves. Facebook stood alone in this
4 regard, with a clear product emphasis on individuals and their connections to others. In 2010, Google,
5 Yahoo, and the other major online advertising sources competed in an entirely different market—one
6 based on search data. The data Facebook had at its disposal was not fungible with search data—it was
7 actionable data about individual users, with their identities fully ascertainable.

8 57. By 2010, Facebook stood alone as the dominant player in the newly emergent market for
9 social advertising—a market in which Facebook’s own users provided Facebook with a constant stream
10 of uniquely valuable information, which Facebook in turn monetized through the sale of advertising.
11 Advertisers, finding no substitute from any other company, paid top dollar for Facebook’s powerful
12 targeting and actionable data, and some of those advertisers—wittingly or not—even fed crucial data
13 about themselves, their products, and the efficacy of their targeting back to Facebook’s network.

14 58. As Facebook itself explained to third-party developers in May 2007, Facebook’s core
15 value proposition and business model was (a) “providing access to a new kind of data—social data, which
16 enables you to build applications that are relevant to users.” With respect to that data, Facebook told
17 developers: “You are on a level playing field with us. You can build robust apps, not just widgets.
18 Complete integration into the Facebook site.” By 2010, it was clear that Facebook’s entire business was
19 selling this new form of “social data” (and machine-learning-driven user targeting based on that data) and
20 that it would do so by selling access to developers and selling advertisements targeting Facebook’s
21 network of engaged and active users.

22 **C. The Data Targeting Barrier to Entry**

23 59. As Facebook’s dominant position emerged in 2010, powerful network effects and
24 feedback loops took hold and solidified that position. Data provided by users, and user targeting based
25 on that data, made Facebook’s network more valuable, thereby attracting more users to the network. As
26 a typical use case, a Facebook user would invite his closest friends and family, who would then invite
27
28

FILED UNDER SEAL

1 and engage with other friends and family members who existed on the network. A familiar feedback
2 loop—a virtuous circle—emerged, rapidly growing Facebook’s user base.

3 60. The content generated by this user base, in turn, increased the value of the Facebook
4 network. With each photograph, relationship status, check-in, or post by a Facebook user, the Facebook
5 network became more valuable, not just as a means of communicating with directly connected
6 acquaintances, but as a means of learning about more remotely connected ones.

7 61. As Samuel Lessin, then Facebook’s VP of Product Management, explained to Mark
8 Zuckerberg in an internal email on October 26, 2012, the data Facebook collects makes Facebook
9 progressively more proficient at collecting and monetizing data:

10 One of the things that puts us currently in a very defensible place is the
11 relationship we have created between the people using Facebook all the
12 time, and us having the information we need to make Facebook a better
13 product. This is the fundamental insight in something like coefficient. *We*
14 *know more about what people want to see because people look at more*
15 *stuff on our platform.* In this respect, while there are other ways to get
close, it feels viscerally correct that there is an ROS dynamic at play, *the*
16 *more people that use the system, the more information we have on how*
17 *to make more people use the system.*

18 (emphasis added).

19 62. A barrier to entry emerged from this feedback loop. To compete with Facebook, a new
20 entrant would have to rapidly replicate both the breadth and value of the Facebook network—a task a
21 mere clone of that network could not accomplish. Indeed, to compete with Facebook, a competitor would
22 not only have to build its own vast network but would have to draw active social engagement on a massive
23 scale—which likely would require drawing a vast quantity of Facebook users away from that platform.

24 63. The costs to switch would be massive: an entrant-competitor would have to present an
25 overall value proposition to users that not only exceeded that of Facebook’s entrenched network, but did
26 so handily. Moreover, to compete with Facebook’s virtuous circle, the value delivered by an entrant-
27 competitor platform would have to facilitate social data mining, including through machine learning and
28 artificial intelligence, that would create even more value for users, developers, and advertisers. This
barrier to entry is referred to throughout this Complaint as the Data Targeting Barrier to Entry (“DTBE”).

FILED UNDER SEAL

64. The DTBE protects Facebook's ability to control and increase prices in the Social Advertising Market without the pressures of price competition from existing competitors or new entrants. Because of its monopoly power in the Social Advertising Market and the DTBE, Facebook has been able

Figure 1: Retail Facebook CPM, Q4 2012 – Q4 2013



to consistently increase the price it charges for social advertising. And this is exactly what Facebook has done since it obtained its dominant position in 2010.

65. From 2011 to 2012, for example, Facebook massively increased the prices it charged for its advertisements—one of the primary sales channels for its social data. That year, costs per thousand impressions (CPM) on Facebook increased by 41%, with a 15% increase in the last quarter of 2011 alone. Cost per click (CPC), which is a measure of advertising costs paid on a by-click basis, rose 23% that same year. Facebook increased prices for social advertising as it also grew the number of advertisements it displayed on its site, indicating monopoly power in the Social Advertising Market.

66. Facebook maintained that power over its prices through 2013, with a 2.9x increase in CPMs year over year. The increase came as overall advertising revenues increased yet again—that year by a staggering 83% over the last.

67. These price increases would not be possible without the DTBE. If a rival network existed with comparable social data available for sale through advertising, Facebook's price increases would have been met with customer migration to the comparable rival. But Facebook had no such rival and was unfettered in its ability to increase prices, even while rapidly increasing its supply of data for sale through advertisement.

FILED UNDER SEAL

1 68. Once Facebook had achieved dominance in the Social Advertising Market, its position
2 only improved—and became more entrenched. The more advertising Facebook sold, and the more social
3 data Facebook collected and packaged for sale, the more effective Facebook became at selling
4 advertising, targeting users, and commercializing direct access to its users’ social data (*e.g.*, through
5 APIs). This, in turn, made entry by a new rival impossible or prohibitively costly, thereby allowing
6 Facebook to increase prices and make additional investments that deepened the DTBE moat surrounding
7 its business.

8 **D. Google’s Failed Entry into the Social Advertising Market**

9 69. In 2010, Google became desperate to enter the Social Advertising Market. It had tried
10 several times to do so before, but each foray was met with failure. Google’s Orkut social network, which
11 was launched days before Facebook, was quickly overtaken. Wave, Google’s social communication
12 platform, never achieved any traction with users. And Google’s Buzz social network—built on the back
13 of its highly successful Gmail product—imploded quickly in early 2010.

14 70. Google’s next attempt to enter the market attacked Facebook’s functionality head-on,
15 which meant attempting to penetrate the powerful DTBE protecting Facebook’s business. Google made
16 a massive, unprecedented investment of resources into building a product with enough value to lure users
17 away from Facebook’s broad, highly engaged social network.

18 71. In 2010, Google’s Vic Gundotra became the company’s Chief Architect. Gundotra pitched
19 a new social network to Larry Page, Google’s cofounder, who returned as CEO of the company in 2011.
20 Gundotra repeated an ominous refrain, “Facebook is going to kill us. Facebook is going to kill us,” which
21 frightened Page into action.

22 72. Page greenlit a new product, Google+. Initially, Google+ sought to leverage Google’s
23 YouTube product to build its social network, requiring a Google+ account for access to certain key
24 features of YouTube. In the face of significant user resistance, Google backed away from that
25 requirement. Nonetheless, Google attempted, through Google+, to build out a “social graph” that would
26 leverage a common user identity across Google products, including YouTube and Gmail.

FILED UNDER SEAL

73. In early 2011, Google began what insiders now refer to as “the 100-day march” toward launch of Google+. The product Google planned to deliver was, by any fair account, uncannily similar to what Facebook offered in terms of product features and functionality. By the summer of 2011, the planned features for Google+ included a continuous scroll product called the “stream” (a clone of Facebook’s “feed” product); a companion feature called “sparks,” which related the “stream” to users’ individual interests; and a sharing app called “Circles,” a purportedly improved way to share information with one’s friends, family, contacts, and the public at large.

74. Unlike Google’s past products, Google+ was not designed to organically grow and scale from small beginnings. From the outset, Google invested massive amounts of resources to bring a finished, full-scale social network to market. Calling the project “Emerald Sea,” Google conscripted almost all of the company’s products to help build Google+. Hundreds of engineers were involved in the effort, which remained a flagship project for Page, who had recently reassumed the Google CEO role. Google’s Gundotra was quoted explaining that the product that would become Google+ was a transformation of Google itself: “We’re transforming Google itself into a social destination at a level and scale that we’ve never attempted—orders of magnitude more investment, in terms of people, than any previous project.”

75. The amount of resources Google brought to bear stood in stark contrast to its previous attempts at penetrating the Social Advertising Market. Google had dedicated barely a dozen staff members to its previous failed social network product, Buzz. At its peak, Google+ involved 1,000 employees from divisions across the country. Google, for example, ripped out its elaborate internal video conferencing system and forced employees to use the Google+ Hangouts video chat feature, which one internal employee described as “janky.” Employee bonuses were tied to the success of Google+. And the entire project was confined to a level of secrecy never before seen at Google.

76. Google+ was released on June 28, 2011. The product included the “stream,” the “Circles” app, the “Hangout” video chat and messaging product, and a photo sharing product. The resemblance to Facebook was striking. As one internal Google employee commented: “this looks just like Facebook. What was the big deal? It’s just a social network.” Another Google employee was quoted as saying, “All

FILED UNDER SEAL

1 this fanfare and then we developed something that in the end was quite ordinary.” One thing was
2 indisputable: with the release of Google+, Google had challenged Facebook head-on by effectively
3 cloning Facebook’s product.

4 77. Because Google’s user base was already massive, the Google+ product attracted millions
5 of users shortly after launch. But though these users signed up for Google+, Google quickly found out
6 they were not using the product. As one former Google employee explained:

7 It was clear if you looked at the per user metrics, people weren’t posting,
8 weren’t returning and weren’t really engaging with the product. Six months
9 in, there started to be a feeling that this isn’t really working.

10 78. The problem for Google+ was the powerful network effect that reinforced the DTBE that
11 protected Facebook. Google’s clone of Facebook did not present enough new value to overcome massive
12 network-based switching costs—the cost to Facebook users of shifting away from an existing networked
13 product in which the users had actively invested their social data for years.

14 79. Paul Adams, a former Google+ user-experience team member, summed it up succinctly
15 when asked why Google+ had failed:

16 What people failed to understand was Facebook and network effects. . . .
17 It’s like you have this grungy night club and people are having a good time
18 and you build something next door that’s shiny and new, and technically
19 better in some ways, but who wants to leave? People didn’t need another
20 version of Facebook.

21 80. By 2014, Google+ was declared a failure and Gundotra, its founder, eventually left
22 Google. Within just a few years, Google—with all of its resources, developers, and existing user base—
23 failed entirely to overcome the DTBE protecting Facebook. As long as Facebook controlled the data
24 derived from an engaged and active user base, it could continue to keep that user base active and engaged.

25 81. The only way to disrupt this virtuous circle was with a rival product that provided
26 significantly more or different value than Facebook, and that itself was propelled to scale by powerful
27 network effects.
28

FILED UNDER SEAL**II. A THREAT TO FACEBOOK'S MONOPOLY: THE RISE OF SMARTPHONES AND MOBILE APPS****A. The Mobile App Revolution**

82. In 2009 and 2010, as Facebook emerged the undisputed winner of the social media wars, another new market had begun to take hold. The launch of the Apple iPhone in 2007 created a market for a new type of cellular phone: one with a user interface capable of robust Internet connectivity and messaging. No longer constrained by numeric keypads for texting—or clunky, permanent alphanumeric keyboards attached to phones, such as with the Treo or Sidekick cellular phones—the iPhone dynamically displayed a multi-touch keyboard and came equipped with a full-featured web browser that rendered complete web pages.

83. By the summer of 2008, Apple's newest iPhone, the iPhone 3G, was released with onboard GPS and other hardware upgrades. Accompanying the release of the new iPhone was a new store for third-party applications that would run natively on the iPhone: the Apple App Store, which opened for business on July 10, 2008, the day before the release of the iPhone 3G.

84. Developers who launched their third-party applications via the App Store reaped huge rewards. There were approximately 500 apps available at the App Store's initial launch. Games using the iPhones accelerometer became immediate successes, some quickly earning hundreds of thousands of dollars by selling downloads for just a few dollars each. Applications that exploited the new GPS functionality in the iPhone also quickly became popular. By September 2008, the Apple App Store had racked up 100 million downloads, and by 2009, it hit 1 billion. iPhone apps had become a new means to deliver scaled value to countless users. Google also launched what became its Play Store (initially known as Android Market) in 2008. It soon overtook Apple's App Store in terms of overall volume, with 82% growth. The mobile app revolution had begun.

85. Mobile apps rapidly proliferated, with huge opportunities for further growth—as the lion's share of cell phone activity by 2010 had become something other than making phone calls. For example, a 2010 Pew Research survey showed that taking pictures and sending text messages had become the most common uses for cellular phones among adults, with more than a third of adult cell phone users accessing

FILED UNDER SEAL

the Internet, playing games, emailing, recording video, or playing music through their cell phones. At the same time, 29% of adult cell phone users had used a downloaded app.

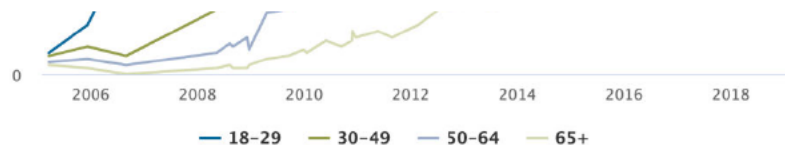
86. A 2010 Nielsen survey showed that games, news/weather, maps and navigation, and social networking were the most popular apps on cellular phones.

87. Notably, mobile apps resonated most strongly with the demographics that had recently adopted social media and were providing their data to Facebook in droves. App users among cell phone

% of adult cell phone users who do each of the following on their phone...

Take a picture	76%
Send or receive text messages	72
Access the internet	38
Play a game	34
Send or receive email	34
Record a video	34
Play music	33
Send or receive instant messages	30
Use an app	29

Source: Pew Research Center's Internet & American Life Project, April 29-May 30, 2010 Tracking Survey. N=1,917 adult cell phone users.



Source: Surveys conducted 2005-2019.

PEW RESEARCH CENTER



Source: The Nielsen App Playbook, December 2009. N=3,962 adults who have downloaded an app in the 30 days prior to the survey.

FILED UNDER SEAL

1 owners were disproportionately younger, with 44% of app users in 2010 under the age of 20 and another
2 41% between the ages of 30 and 49. These were the same demographics that were rapidly adopting social
3 media as part of their lives and providing Facebook with the social data that built and maintained the
4 DTBE that protected its business.

5 88. Many of the mobile apps that were rapidly attracting users were doing so because they
6 presented their own specialized value propositions. These apps had to be specialized because cellular
7 phone screens were smaller, particularly in 2010, and mobile traffic was driven by specialty software,
8 often designed for a single purpose. Users signed up for these apps with their e-mail addresses and
9 personal information and interacted directly with the apps.

10 89. As *Wired* magazine described in 2010, a typical user moved from app to app, each with
11 some specialized use:

12 You wake up and check your email on your bedside iPad—that's one app.
13 During breakfast you browse Facebook, Twitter, and the New York
14 Times—three more apps. On the way to the office you listen to a podcast
15 on your smartphone. Another app. At work, you scroll through RSS feeds
16 in a reader and have Skype and IM conversations. More apps. At the end
of the day, you come home, make dinner while listening to Pandora, play
some games on Xbox Live, and watch a movie on Netflix's streaming
service.

17 90. In 2010, Morgan Stanley projected that within five years, the number of users who
18 accessed the Internet from mobile devices would surpass the number who accessed it from PCs. The
19 Internet was at an inflection point—the World Wide Web was no longer the dominant way to access
20 information. Users were obtaining their information from specialized walled gardens, and Facebook's
21 own walled garden was one app away from being superseded.

22 91. The years leading up to 2010 saw the rise of streaming apps, such as Netflix and Pandora,
23 and e-book readers, such as Kindle and iBooks. Apple's 2010 list of top-grossing iPhone apps included
24 mobile games such as Angry Birds, Doodle Jump, Skee-Ball, Bejeweled 2 + Blitz, Fruit Ninja, Cut the
25 Rope, All-in-1 GameBox, the Moron Test, Plants vs. Zombies, and Pocket God. Facebook's mobile app
26
27
28

FILED UNDER SEAL

1 topped the list of free downloads in the App Store, along with Words with Friends, Skype, and the
2 Weather Channel App.

3 **B. Facebook Recognizes the Looming Threat Presented by Mobile Applications**

4 92. By 2011, Facebook realized that it had fallen behind. Facebook had just debuted its new
5 “Timeline” product, a controversial modification of the Facebook feed that generated dynamic content
6 for each user rather than a static series of posts visible to the user. Facebook had spent the last eight
7 months prioritizing its desktop experience and its new Timeline product. But while it did so, mobile
8 applications continued their meteoric rise.

9 93. Facebook’s own mobile application was built on a technology called HTML5, which at
10 the time was good for building web pages but not for building mobile apps native to iOS and Android
11 smartphones. As a result, Facebook’s mobile app was buggy, prone to crashes, and painfully slow. As
12 Zuckerberg would lament years later about HTML5, “We took a bad bet.”

13 94. Zuckerberg reflected in 2018 that Facebook had fallen behind when mobile apps emerged:

14 One of my great regrets in how we’ve run the company so far is I feel like
15 we didn’t get to shape the way that mobile platforms developed as much as
16 would be good, because they were developed contemporaneously with
17 Facebook early on. I mean, iOS and Android, they came out around 2007,
18 we were a really small company at that point—so that just wasn’t a thing
19 that we were working on.

20 95. As mobile apps rose, Facebook’s desktop product acquired users at a slower pace. All of
21 this occurred as Facebook was planning its initial public offering. Facebook knew that its position was
22 eroding and that if mobile growth continued, its IPO debut would be in the midst of material changes to
23 its business, undermining Facebook’s financial and qualitative disclosures to public investors.

24 96. But there was no avoiding the issue. Facebook held its IPO on May 18, 2012. By the time
25 Facebook released its first annual report, the trend was unmistakable—the transition to mobile devices
26 from desktop web-based applications posed an existential threat to Facebook’s business. In its 2012 Form
27 10-K, Facebook disclosed this risk to shareholders as one of the factors that affected its bottom line:
28

FILED UNDER SEAL

Growth in the use of Facebook through our mobile products as a substitute for use on personal computers may negatively affect our revenue and financial results.

We had 680 million mobile MAUs in December 2012. While most of our mobile users also access Facebook through personal computers, we anticipate that the rate of growth in mobile usage will exceed the growth in usage through personal computers for the foreseeable future and that the usage through personal computers may decline or continue to decline in certain markets, in part due to our focus on developing mobile products to encourage mobile usage of Facebook. For example, during the fourth quarter of 2012, the number of daily active users (DAUs) using personal computers declined modestly compared to the third quarter of 2012, including declines in key markets such as the United States, while mobile DAUs continued to increase. While we began showing ads in users' mobile News Feeds in early 2012, we have generated only a small portion of our revenue from the use of Facebook mobile products to date. In addition, we do not currently offer our Payments infrastructure to applications on mobile devices. If users increasingly access Facebook mobile products as a substitute for access through personal computers, and if we are unable to continue to grow mobile revenues, or if we incur excessive expenses in this effort, our financial performance and ability to grow revenue would be negatively affected.

C. The Facebook Platform

97. Although Facebook faced a looming threat from mobile applications, it maintained an important source of leverage: its social data. Facebook possessed (and continued to receive) vast quantities of information about its massive user base, including how each user was connected to others. This information was valuable to both new and existing mobile applications, which could leverage Facebook's social data to obtain new users and to build novel social features, functions, and apps.

98. Facebook referred to its network as its "Graph," coined after a mathematical construct that models connections between individual nodes. The Facebook Graph contained user "nodes," with connections and information exchanged among nodes as "edges." Facebook coined the term "Open Graph" to describe a set of tools developers could use to traverse Facebook's network of users, including the social data that resulted from user engagement.

FILED UNDER SEAL

1 99. Importantly, Open Graph contained a set of application programming interfaces (“APIs”)
2 that allowed those creating their own social applications to query the Facebook network for information.
3 As Facebook explained in its 2012 Form 10-K:

4 ***Open Graph.*** Our underlying Platform is a set of APIs that developers can
5 use to build apps and websites that enable users to share their activities with
6 friends on Facebook. As Open Graph connected apps and websites become
7 an important part of how users express themselves, activities such as the
8 books people are reading, the movies people want to watch and the songs
9 they are listening to are more prominently displayed throughout
Facebook’s Timeline and News Feed. This enables developer apps and
websites to become a key part of the Facebook experience for users and
can increase growth and engagement for developers.

10 100. Open Graph, along with other Facebook products, such as its NEKO advertising and
11 Payments products, comprised Facebook’s Platform. The Platform was vital to Facebook’s business
12 because it ensured that engagement continued on Facebook. Without the Platform, Facebook would be
13 required to build applications that increased the value of its network itself—meaning that Facebook would
14 have to try to predict what applications users wanted; design, code, and scale those applications across
15 its user base and network; and bear the risk and resource drain of guessing wrong and making mistakes.

16 101. Facebook did not have the resources to do this, so it decided instead to allow third parties
17 to build applications for the Platform. As Mark Zuckerberg observed in a February 2008 email to
18 Facebook’s VP Engineering for Platform Michael Vernal, a senior Zuckerberg lieutenant who was in part
19 responsible for creating Open Graph:

20 Platform is a key to our strategy because we believe that there will be a lot
21 of different social applications And we believe we can’t develop all
22 of them ourselves. Therefore It’s important for us to focus on it
23 because the company that defines this social platform will be in the best
position to offer the most good ways for people to communicate and
succeed in the long term.

24 102. Put simply, Facebook could either speculate on new social applications by building them
25 itself or it could provide a platform for others to do so. For years, Facebook opted to provide a platform
26 until it was able to develop its own social applications.

FILED UNDER SEAL

1 103. But Facebook also recognized that developers on its Platform could potentially pose a
2 competitive threat. In its 2012 annual report, Facebook disclosed the following significant risk factor to
3 its operations:

4 In addition, Platform partners may use information shared by our users
5 through the Facebook Platform in order to develop products or features that
6 compete with us. . . . As a result, our competitors may acquire and engage
7 users at the expense of the growth or engagement of our user base, which
8 may negatively affect our business and financial results.

9 104. Thus, Facebook knew that competition could come from its own third-party application
10 developers. But Facebook nevertheless actively sought developers to build applications on its Platform
11 because of the potential to extract profits from the applications these developers built and the users they
12 attracted to, and engaged on, Facebook's network.

13 105. As Facebook explained to its investors in 2012, maintaining a Platform on which
14 developers could build applications meant more engagement and therefore greater ad revenues for
15 Facebook:

16 Engagement with our Platform developers' apps and websites can create
17 value for Facebook in multiple ways: our Platform supports our advertising
18 business because apps on Facebook create engagement that enables us to
19 show ads; our Platform developers may purchase advertising on Facebook
20 to drive traffic to their apps and websites; Platform developers use our
21 Payment infrastructure to facilitate transactions with users on personal
22 computers; Platform apps share content with Facebook that makes our
23 products more engaging; and engagement with Platform apps and websites
24 contributes to our understanding of people's interests and preferences,
25 improving our ability to personalize content. We continue to invest in tools
26 and APIs that enhance the ability of Platform developers to deliver
27 products that are more social and personalized and better engage people on
28 Facebook, on mobile devices and across the web.

106. Facebook's Platform was valuable to Facebook in several important ways.

107. First, the Platform meant that new applications would be built on Facebook's network,
increasing the value of Facebook's network as the applications became more popular. The increased
engagement with Facebook as a result of these new applications translated to better-targeted content and
higher advertising revenues.

FILED UNDER SEAL

1 108. Second, Facebook would not need to spend significant resources to develop new
2 applications or test new business models—third parties would do that instead. Facebook could merely
3 wait for an application built for its Platform to gain widespread adoption, then either build a competing
4 application or passively glean the benefits of that popular application’s user engagement, including
5 valuable new social data for Facebook and its network.

6 109. Third, access to Facebook’s network was itself valuable to third-party developers, so
7 Facebook could charge developers—most notably, through API access and advertising purchases—to
8 access Facebook’s Platform and the social data it collected from Facebook’s massive number of engaged
9 users.

10 **D. The Profitable Open Graph Platform and Mobile Install Business**

11 110. Facebook continued to struggle to catch up with the new onslaught of mobile applications,
12 but it recognized that the new apps required aggressive user growth to be profitable. Among other things,
13 Facebook’s APIs allowed mobile app developers to query the friends of a person’s friends, which allowed
14 mobile applications to find other users who might be interested in using their apps.

15 111. Mobile apps also could use Facebook to communicate across Facebook’s network, either
16 directly with a user’s friends or with others not directly connected with the user. A mobile payment
17 application, for example, could enable two strangers to pay each other, even if they were not directly
18 connected on Facebook—so long as both of them existed somewhere on Facebook’s Platform. A user of
19 a dating application, such as Tinder, could use Facebook’s APIs to find a compatible date, either in the
20 extended network of one’s friends or beyond—anywhere on Facebook’s Platform.

21 112. Facebook quickly realized it could monetize the value of its network through third-party
22 mobile applications, and it moved aggressively to do so, beginning with games built to run on Facebook’s
23 Platform. Those games, many of which were social games that allowed users to play with and against
24 each other, sought above all else new users to increase their adoption. Facebook’s Vernal sought to obtain
25 a beachhead with these applications, monetizing each additional game install that resulted from the use
26 of Facebook’s Platform or from Facebook’s advertising product, NEKO.

FILED UNDER SEAL

113. For example, Facebook included ads as “stories” on user timelines that indicated whether the user knew other users who were playing a particular game. Facebook then monetized such advertisements when the game obtained new users from them. As Vernal explained in a May 2012 e-mail:

The biggest/most efficient market segment for advertising on mobile today is driving app installs. This is at least partly because it’s the most measurable—if you know that you get \$0.70 from every game you sell, then in theory you can afford to pay up to \$0.69/install. This kind of measurability allows for maximal bidding.

So, what we’re trying to do is kickstart our sponsored stories business on mobile by focusing on one particular type of story (is-playing stories) and one market segment (games), make that work really well, and then expand from there.

114. Facebook thus leveraged its most valuable asset—the information it had about its users, their interests, and most importantly, their friends—to make money from the proliferation of mobile games.

115. Games like Farmville, a mobile application that allowed players to create their own simulated farms, quickly took off because of Facebook’s Platform. Facebook increasingly recognized that it could obtain engagement from users through the game itself.

116. This strategy led to a broader one, in which Facebook drove app installs by allowing developers to advertise to its user base and traverse Facebook’s social network through the Facebook APIs. Facebook collected a fee for each app install that resulted from its network. Vernal outlined the plan in detail:

Roughly, the plan:

1/ Create new iOS + Android SDKs, because the current ones are terrible. Ship Thunderhill so we get even broader adoption of our stuff.

2/ Wire them up to make sure we know when you’re playing a game (so we can generate the same kind of is-playing stories we can on canvas).

3/ Generate a bunch of effective, organic distribution for these games via our existing channels (news feed, net ego on both desktop + mobile). Ship

FILED UNDER SEAL

1 send-to-mobile, which allows us to leverage our desktop audience to drive
2 mobile app traffic.

3 4/ Create an even better app store than the native app stores (our app center)
4 and make a lot of noise about it, so developers know that they should be
5 thinking about us to get traffic to their mobile apps.

6 5/ Introduce a paid offering, probably cost-per-install (CPI) based, where
7 you can pay us to get installs from your mobile app. Primary channels for
8 this paid distribution are News Feed and App Center (on desktop + mobile)
9 as well as RHC on desktop.

10 117. The strategy was clear, not just for gaming, but for mobile apps. Facebook would make
11 money by allowing app developers to leverage its user base. Facebook would advertise social games to
12 its users by plumbing their social data—including data about when they played games and which of their
13 friends played them—and in exchange, Facebook would receive some amount of money per install, which
14 would be the app developer's cost-per-install (CPI). The same plan would work for mobile applications
15 generally.

16 118. By the end of 2011 and the beginning of 2012, Facebook began discussing other ways to
17 monetize its Platform, including its Open Graph APIs. One way was to sell API access based on usage.
18 Zuckerberg and top executives at Facebook extensively debated a tiered approach to API access.
19 Facebook deliberated over a pricing model for API access, and internally decided that it would be possible
20 to sell API access to third-party developers. Facebook also decided that it could bundle API access with
21 the ability to advertise on Facebook. However, as explained below, Facebook gave up the profits it could
22 glean from API access for the chance to dominate the Social Advertising Market entirely, excluding
23 competitors (both actual and potential) and leveraging network effects to achieve and maintain monopoly
24 power.

25 **III. FACEBOOK WEAPONIZES ITS PLATFORM TO DESTROY COMPETITION**

26 **A. Facebook Makes Plans to Remove Vital Platform Functionality and Refuses to Sell 27 Social Data to Competing Application Developers**

28 119. Although Facebook had made significant amounts of revenue and profit selling access to
its social data through its APIs and its NEKO advertising system and had planned to expand that business,
it chose not to, sacrificing those significant profits.

FILED UNDER SEAL

1 120. By the end of 2011 and the beginning of 2012, Zuckerberg along with Facebook's Vice
2 President of Growth, Javier Olivan, its VP of Product Management, Samuel Lessin, and Michael Vernal
3 internally debated a plan to prevent third-party developers from building their own competing social
4 networks that could be capable of generating engagement and social data independent of Facebook's
5 Platform.

6 121. Emerging mobile applications such as Line, WeChat, and Instagram were creating their
7 own vast user bases with identity and login features separate from the Facebook Platform. Their
8 increasing ubiquity posed an existential threat to Facebook's core business, which relied heavily on
9 engagement from its user base. These applications provided quintessentially social applications, such as
10 image sharing, messaging, and payments—a direct threat to Facebook's own applications, including
11 Facebook's own fledgling Messenger application.

12 122. Mobile applications were rapidly eating away at Facebook's dominance, which relied
13 heavily on its web-based desktop product. Zuckerberg openly acknowledged that its desktop applications
14 were not the future and that native phone apps would dominate the mobile web in the future.

15 123. Zuckerberg therefore sought to consolidate core applications into its own centralized
16 Facebook application, noting in a March 2012 Q&A with employees that Facebook was “building
17 towards social Facebook versions where you can use the individual app or the Facebook version.” That
18 is, users could “replace whole parts of your phone with these Facebook apps and [they] will be a whole
19 package for people.”

20 124. Beginning in the fall of 2011 and well into 2012, Mark Zuckerberg and his chief
21 lieutenants, Lessin and Vernal, planned to address the looming mobile applications threat. Their solution
22 was a scheme to disrupt the massive growth of mobile applications by attracting third-party developers
23 to build for Facebook's Platform and then remove their access to the APIs that were most central to their
24 applications. They would accomplish this by leveraging Facebook's “Friends” and “Timeline” APIs, as
25 well as other vital APIs, including those relating to messaging.

26 125. The Friends APIs let third-party developers traverse the Facebook Graph, searching
27 through a user's friends as well as the friends of their friends. Zuckerberg and his executives proposed
28

FILED UNDER SEAL

1 modifying the APIs to deny third-party developers access to information about a user's friends (and the
2 friends of their friends) unless that developer's application was already installed by a user's friends to
3 begin with. This ensured that new applications could not obtain new users or use Facebook's social data
4 to increase the value of their application.

5 126. Facebook also foreclosed developers from continuing to extract information about a user's
6 friends from their timeline or news feed. Thus, third-party applications that relied on the stream of
7 information that flowed through a user's news feed, such as a post about a friend of the user getting
8 engaged or sharing a news article, would be abruptly left with none of the social data they needed to
9 function.

10 127. In 2013, Facebook extended its API "reciprocity" plan to encompass its Events API, a
11 group of endpoints and permissions relating to live events and ticketing that were being actively used by
12 5,300 applications on the Facebook Platform.

13 128. Removing access to these APIs halted the growth of tens of thousands of third-party
14 applications that relied on these essential APIs and were, in Facebook's view, threatening Facebook's
15 dominance by eroding the DTBE that protected Facebook's business.

16 129. Facebook's plan prevented any competitive third-party application from buying social
17 data from Facebook, either through its Platform APIs or through its advertising Platform. As Vernal
18 explained to Lessin in August of 2012, Facebook would "not allow things which are at all competitive to
19 'buy' this data from us."

20 130. Facebook thus refused to sell its social data to any competitive third-party developer,
21 sacrificing significant short-term profits in exchange for a competitive advantage in the Social
22 Advertising Market. If not for the prospect of driving these competitors out of the markets in which
23 Facebook competed, the decision to refuse to sell social data to third-party developers made no economic,
24 technical, or business sense.

25 131. Third-party developers with successful applications increased the value of Facebook's
26 overall network by increasing engagement and generating the very social data Facebook sold through its
27 targeted advertising channels, including to developers. As Zuckerberg had observed years earlier,
28

FILED UNDER SEAL

Facebook itself could not broadly develop new third-party apps or anticipate what apps would be successful, so it relied on third parties to do so. Refusing API and social data access to third parties meant that they could not develop the applications that were vital to Facebook's growth, engagement, and advertising revenue. Facebook decided to deliberately sacrifice the value its third-party developers provided to secure dominance in the Social Advertising Market.

B. Facebook's Social Data Heist

132. In May 2012, Zuckerberg decided to use the threat of blacklisting from its Platform to extract precious social data from some of Facebook's competitors. He instructed his executives to quietly require "reciprocity" from major competitors that used Facebook's Platform. The reciprocity Zuckerberg demanded was the very lifeblood of these competitors' businesses—the social data harvested from user engagement on their competing networks.

133. By the middle of 2012, Facebook began to block some of its competitors from using its Platform and thereby obtaining Facebook's social data. Facebook had already blocked Google, including its competing social network Google+, from access to Facebook's APIs and advertising platform. With respect to Twitter, Instagram, Pinterest, and Foursquare, Facebook would demand "reciprocity" or blacklist them. Reciprocity, of course, meant that these competing social networks would have to hand over their most valuable asset—their social data—to their rival Facebook.

134. If rivals did not comply with Zuckerberg's demands to hand over their social data to Facebook, Facebook would simply take it. In May 2012, Vernal directed his subordinates, Douglas Purdy (Director of Engineering for Platform) and Justin Osofsky (VP of Global Operations), to build "our own hacky scraper" and a "bunch of scrapers" to crawl rival sites like Twitter and Instagram and harvest their social data—with or without their consent. If Twitter or Instagram refused to agree to Zuckerberg's "reciprocity" proposition, Facebook would use the scrapers to obtain the data instead.

135. In August 2012, Facebook considered broadening its list of companies to shake down for social data—or to block entirely from Facebook's Platform. That month, Facebook's then VP of Business and Marketing Partnerships, David Fischer identified other potential product categories and competitive companies in each category to block:

FILED UNDER SEAL

I'd expect that a large part of the market for our network will come from current and potential competitors. Here's the list that Jud worked up of what we'd likely prohibit if we were to adopt a ban on "competitors" using a broad definition:

- Social network apps (Google+, Twitter, Path, etc.)
- Photo sharing apps (Picasa, Flickr, LiveShare, Shutterfly, etc.)
- Messaging apps (WhatsApp, Viber, Imo, KakaoTalk, etc.)
- Local apps (Google+ local, Google Offers, Yelp, yp, etc.)
- Social search apps (HeyStaks, Wajam, etc.)
- Platforms (Google Play, Amazon, etc.)

136. Facebook thus identified its direct, horizontal competitors for social data, including those competitors that had, or could create, rival social advertising platforms. These categories of competing applications, particularly on mobile platforms, threatened Facebook's business because they created social networks independent of Facebook, each capable of generating their own valuable social data. If Facebook lost control over these companies, it would lose access to the social data they generated, which meant Facebook's own product could not drive engagement and sell advertising. This was because Facebook's machine-learning algorithms—used to target users for advertising and content, including by granular demographics—required social data to function.

137. In August 2012, Facebook gave a presentation to its Board of Directors that included various revenue models to monetize its Platform, including its APIs. The Board understood that Facebook could monetize its Platform by charging per company, per application, per user, or per API call.

138. But Facebook opted to do none of those things. Instead, it decided to sacrifice those profits in the short term to obtain complete control over the growing mobile application and advertising markets, thereby maintaining and furthering its dominance of social data and the Social Advertising Market.

139. Facebook's plan was to instead block competitors from using its Platform, thereby preventing them from eroding the DTBE that protected Facebook's business. In the case of a select few companies with social data that Facebook needed to maintain and grow its own business, however, Facebook would coerce them into agreements to share their most valuable social data with Facebook. If

FILED UNDER SEAL

1 they refused, Facebook would blacklist them and take it from them anyway with its own crawling
2 software that would scrape their public-facing site for information.

3 140. In September 2012, Zuckerberg formalized his order to shut down the Friends and News
4 Feed/Timeline APIs and to coerce rivals into providing their valuable data to Facebook on pain of
5 blacklisting. On October 30, 2012, Vernal notified his subordinates of Zuckerberg's decision:

6 We are going to dramatically reduce the data we expose via the Read API
7 We are going to change friends.get to only return friends that are also
8 using the app Since friends.get will only return other TOSed users'
9 data [data from users that agreed to an application's terms of service], that
10 means we no longer need the friends_* permissions. We are going to
11 remove/whitelist access to the Stream APIs [the News Feed API]. We are
going to limit the ability for competitive networks to use our platform
without a formal deal in place We are going to require that all platform
partners agree to data reciprocity.

12 141. This decision meant several things: (1) when a third-party application called the Friends
13 APIs, it could not obtain information about a user's other friends unless those friends already had installed
14 the application; (2) the News Feed APIs would no longer provide information about a user's connections;
15 (3) access to those API could be "whitelisted" for third-party developers that were offered—and agreed
16 to—data reciprocity; and (4) reciprocity would be required for any access to the APIs.

17 142. In November 2012, Osofsky, who was then head of Facebook's Platform, summarized the
18 policy changes required by the decision:

19 Policy changes: define competitive networks + require they have a deal
20 with us, regardless of size. Maintain size-based thresholds for all other
21 developers to force business deals. Require data reciprocity for user
extended info to ensure we have richest identity.

22 143. Facebook knew that these changes would eliminate the "growth channel used by 23% of
23 all Facebook apps" and that 89% of the top 1,000 iPhone apps relied on the full friends list API, with
24 75% of the top 1,000 iPhone apps relying on the Friends permissions APIs. Facebook determined that
25 popular applications on its platform with millions of customers would break as a result of the decision,
26 including FarmVille, ChefVille, CityVille, Skype, Spotify, Xobni, Texas Holdem, Yahoo, Trip Advisor,
27 Microsoft's Birthday Reminders, Samsung's clients, Glassdoor and dozens of others.
28

FILED UNDER SEAL

144. On November 19, 2012, Zuckerberg broadly announced his decision to block competitors or require full data reciprocity for continued access. Facebook's COO Sheryl Sandberg immediately ratified the decision, adding that "we are trying to maximize sharing on Facebook, not just sharing in the world," with the note that the distinction was a "critical one" and the "heart of why."

145. Facebook began preparing its 2013 plan for its mobile advertising business, which included the launch of a new version of its Platform, version 3.0. Platform 3.0 would (according to Facebook) facilitate Facebook's transition from its desktop advertising business to a mobile advertising business. A central element of the transition plan was the implementation of Zuckerberg's decision to remove the Friends and News Feed APIs.

146. Vernal explained Zuckerberg's decision to other Facebook employees in November 2012, noting that he believed the amount of data that Facebook required from competitors was "crazy":

[A company must share] every piece of content by that user that can be seen by another user. What Mark is saying is he wants certain partners (I assume not all) to give us news feeds on behalf of their users, which is kind of crazy.

147. Facebook continued to formalize its plan to require the right to crawl the sites of its competitors as a condition of access to its Platform. In November 2012, Facebook's Group Product Manager, Rose Yao explained the scheme:

We also reserve the right to crawl a partner website for the user's data. Partners cannot blacklist or block Facebook from crawling your site or using the API. If they do, Facebook reserves the right to block the partner from using our APIs The theory behind Action Importers was that we needed to balance the leverage. You can call our APIs and access our data, as long as we can call your APIs (if you have them) or crawl your web site (if not) and access your data. It's one thing to drag your heels, but if we're the ones doing the work then we force you to make a decision—either you allow us access to your data, or you block us. If you block us, then it's really easy/straightforward for us to decide to block you. What's changed? ***When we first started discussing this, we were talking about doing this only for top partners. I think a lot of folks interpreted this as just a negotiation tactic—we'd just threaten to do this if they didn't cooperate. What's changed between then and now is that this is now very clearly not a negotiation tactic—this is literally the strategy for the read-side platform.***

FILED UNDER SEAL

1 (emphasis added).

2 148. Thus, what began as a negotiation strategy to extract social data from rivals became the
3 foundation of Facebook's Platform strategy. For competitors that posed enough of a threat to create their
4 own rival network, Facebook required them to hand over the only leverage they had—the social data they
5 derived from their users' engagement.

6 149. For some rivals that directly competed, no amount of data would justify access to
7 Facebook's Platform, and for nascent threats that relied on Facebook's platform that did not have any
8 useful data to extract, Facebook's decision was to simply cut off their access to the Friends and News
9 Feed APIs, killing their businesses almost immediately.

10 150. Vernal expressed concern about the strategy to Zuckerberg in November 2012, noting that
11 he was skeptical that competitors such as Pinterest would allow Facebook to take their social data. If they,
12 as well as others, did, Facebook would become a central exchange for data collected among competitors.
13 That is, competitors would share the data to Facebook and Facebook would then share that data back to
14 the competitors that participated in the scheme. *Facebook would become a data-passthrough*
15 *mechanism.*

16 151. In December 2012, despite recognizing that API access, particularly when bundled with
17 Facebook's NEKO advertising platform, was profitable, Facebook decided not to charge for API access
18 and began full implementation of Zuckerberg's decision.

19 152. Although Facebook had planned to announce its decision not to allow access to Friends
20 data through its Friends and News Feed APIs in a public blog post, Zuckerberg vetoed that decision in
21 December 2012. Instead, Zuckerberg decided to enforce the decision selectively and covertly after
22 deliberately analyzing Facebook's competitors. Some competitors would be blocked entirely from the
23 APIs, while some select few would be blocked only if they did not provide their own social data to
24 Facebook.

25 **C. Facebook Targets Its Competitors for Reciprocity or Denial of API Access**

26 153. Beginning in January 2013, Facebook began an internal audit of all of the applications that
27 relied on its Platform. It immediately identified competitors to shutdown entirely from accessing
28

FILED UNDER SEAL

Facebook's APIs or advertising platform. Specifically, Zuckerberg ordered that WeChat, Kakao, and Line be restricted from using the Friends and News Feed APIs and even from advertising on Facebook's NEKO and other platforms.

154. Facebook's David Fischer balked at the decision, noting that blocking competitors even from the advertising platform was irrational and unworkable:

I continue to believe we should allow ads from competitors for several reasons: We should be secure enough in the quality of our products to enable them to compete effectively in the open marketplace It looks weak to be so defensive. This will be a challenge to enforce. We have many competitors and the list will grow in time. How will we judge retailers and e-commerce sites as we grow Gifts, since they arguably are competitors too?

155. Fischer was right. The decision made no rational economic or business sense. The sole purpose of refusing to sell social data as part of the Facebook Platform or through advertising was to shut out competition and allow Facebook to dominate the Social Advertising Market. Aside from that anticompetitive purpose, the decision to refuse to sell social data or advertisements even at full price was so facially irrational that Facebook's own employees who may not have been fully privy to the anticompetitive scheme protested at the irrationality of the decision.

156. That same month Facebook's Osofsky pleaded with Vernal to make an announcement that would send a clear signal to developers, but Vernal responded that Zuckerberg had already rejected that approach. As Vernal explained, telling developers about the decision means bearing the "very real cost" of "changing the rules," including the "PR cost" of betraying developers that Facebook had induced to build for Facebook's APIs and Platform.

157. That same month, Facebook continued to implement Zuckerberg's decision to blacklist competitors. He ordered that Facebook competitor Vine be "shut down" from Facebook's API and Platform, including from advertising. Facebook had again sacrificed the profits it would glean from increased engagement and advertising revenue as a result of Vine's use of Facebook's Platform in exchange for the exclusion of Vine from the competitive landscape.

FILED UNDER SEAL

1 158. Indeed, Facebook’s mobile advertising platform was growing rapidly, and blocking large
2 companies from using it made no economic sense other than to effectuate Zuckerberg’s scheme to prevent
3 rivals from competing with Facebook. In a January 20, 2013 email, Facebook’s then-Director of Product
4 Management and Platform Monetization team, Deborah Liu reported: “Neko grew another 50% this
5 week! Hit a high of \$725k Friday (see charge below). We are now 5% of total Ads revenue and 21% of
6 mobile ads revenue.”

7 159. Lessin responded to the news: “The neko growth is just freaking awesome. Completely
8 exceeding my expectations re what is possible re ramping up paid products.”

9 160. Liu was clear, however, that the increased revenues occurred notwithstanding the
10 blacklisting of formerly large spenders, such as WeChat: “WeChat and other competitive networks are
11 no longer advertising on Neko based on policy.”

12 161. In February of 2013, Facebook shut down Yahoo!’s access to key APIs, resulting in direct
13 negotiations between Yahoo!’s Marissa Mayer and Facebook’s Sheryl Sandberg in order to restore
14 Yahoo!’s access to the Facebook Platform.

15 162. In March 2013, Facebook’s key Platform employees began to voice concern that the
16 approach taken by Facebook of shutting down access and then coercing “data reciprocity” was
17 problematic. They instead encouraged making an upfront announcement that the APIs would be
18 unavailable and then negotiating a deal for access to Facebook’s Platform. In an e-mail that month from
19 Purdy to other Facebook employees and executives, he wrote:

20 I have been thinking about the challenges around reciprocity and
21 competitive enforcement (friends.get, etc.) and fact that *it is all post facto*.
22 The way we are structured today, you build an app on FB and then launch
23 and then we may just shut you down, harming users and the developer. I
24 wonder if we should move as quickly as possible to a model in product
25 where all you get from platform is login (basic info) and sharing without
26 approval. All other APIs are available in development, but have to be
27 approved before the app launches to real users (basically all apps using
28 friends.get have to have that capability approved). We are roughly on
course to deliver this as part of unified review, save for the more granular
approval for things like friends.get? What I love about this too is we could
make our whitelists so much cleaner by making each capability an approval
thing. Marie: I think makes your “deprecations” much easier. Thoughts?

FILED UNDER SEAL

1 163. Although Facebook moved towards full deprecation of the APIs with the exception of
2 those with whitelisting agreements, it continued its campaign of quietly shutting down competitors'
3 access to the APIs and then asking them to make a reciprocity deal. Indeed, Facebook soon thereafter
4 shut down three competing Amazon apps, resulting in Amazon protesting that the decision “will break
5 of our live integrations.”

6 164. That same March in 2013, Facebook used API and Platform access as leverage to acquire
7 rival Refresh.io. Facebook internally decided that it would threaten Refresh.io with denial of access to
8 the APIs unless it sold its business to Facebook. That same form of leverage would be used to acquire
9 other rivals—either they sold to Facebook or they saw their business ejected from Facebook’s Platform.

10 165. In 2013, Facebook also began using mobile spyware company Onavo to secretly track
11 application usage on customers’ phones. Onavo, through deceptive terms of service, tracked app usage
12 in real time, and Facebook used that data to target specific competitors. By April 2013, Olivan was using
13 Onavo to track Snapchat, Pinterest, WhatsApp, Tumblr, Foursquare, Google, Path, vine, Kik, Voxer,
14 MessageMe, Viber, GroupMe, Skype, Line, and Tango. One internal Olivan presentation contained
15 detailed usage data for these applications from August 2012 to March 2013.

16 166. By July 2013, Onavo data was providing detailed intelligence to Facebook on 30 million
17 Onavo users. Among all of the apps, the data showed the meteoric rise of WhatsApp, a direct competitor
18 to Facebook’s own fledgling product, Messenger.

19 167. Armed with detailed intelligence about its competitors—both on and off the Facebook
20 Platform—Facebook ordered a detailed audit of Facebook applications that relied on the Friends and
21 News Feed APIs.

22 168. Facebook’s Director of Developer Platforms & Programs, Konstantinos Papamiltiadis,
23 reported back that there were 40,000 apps using the APIs that were to be restricted, with 7% of them
24 being photo or video sharing apps.

25 169. Facebook then began to categorize these third-party applications into three general
26 categories: (1) developers that “may cause negative press” if their access to APIs were shut down; (2)
27 applications that “provide strategic value”; and (3) applications that were “competitive” or “not useful to
28

FILED UNDER SEAL

1 FB. Application developers that would experience “a Major Business Disruption/Kill” as a result of the
2 restriction of API access received a “PR flag.”

3 170. In response to the categorization, Lessin immediately ordered his subordinates to “shut
4 down access to friends on lifestyle apps . . . because *we are ultimately competitive with all of them.*”
5 (emphasis added).

6 171. As Facebook continued its analysis of the applications that relied on the Friends and News
7 Feed APIs, it became clear that Facebook’s plan would result in the deprecation of the “majority of the
8 API surface”—namely, the APIs that were the most essential parts of the Facebook Platform.

9 **D. Facebook Decides to Add the Events API to Its Reciprocity Scheme**

10 172. In February 2013, Facebook internally decided to begin “Scaling Event Advertising.”
11 However, in order to target social advertising in this area, Facebook’s systems would need to ingest large
12 quantities of accurate events and ticketing data. (*See* PALM-004809292; PALM-001336845.)

13 173. By Summer 2013, Facebook was ready to move forward with a plan to supplement identity
14 information and scale events-focused social advertising by using location, intent, and transaction data
15 typically within the hands of live ticketing and events aggregators and merchants. (PALM-010304019.)

16 174. A team of Facebook Platform Partnership employees including Rob Daniel, Jackie Chang,
17 Simon Cross, and Ime Archibong initially attempted to acquire this data straightforwardly from various
18 brokers and ticket vendors, including TMS, SongKick, and EventSource. However, Facebook’s efforts
19 were rebuffed or met with prohibitively expensive monetary demands. (*See, e.g.*, PALM-010304019 (five
20 thousand dollars a month just for “movie time and location data” from TMS).)

21 175. In Autumn of 2013, Facebook settled upon a new tactic to acquire events-related social
22 data: expanding its reciprocity scheme to encompass the Events API.

23 176. The Events API comprised a collection of endpoints, groups, and permissions in Graph,
24 Rest, and FQL that allowed Platform developers to publish events to Facebook, to view Event Pages on
25 Facebook, and to view a list of Facebook Events joined by an application’s users and that user’s friends
26 (among other things). On October 8, 2013, Facebook Product Manager Eddie O’Neil reached out to
27 engineer Dev Chakravarti to inquire about who was using the Events API and whether it could be
28

FILED UNDER SEAL

1 deprecated as part of the PS12n initiative. Chakravarti—apparently confused by the whole line of
2 questioning—was directed by O’Neil to Simon Cross, who was at that time handling Facebook’s effort
3 to acquire events-related social data to bootstrap events-focused ad targeting. O’Neil then sent
4 Chakravarti information about “Platform Simplification (PS12n),” among other links. (See PALM-
5 000721698, at 701-02.)

6 177. Over the next week, O’Neil and Chakravarti corresponded about technical issues
7 regarding the Events API. O’Neil made clear that Chakravarti was to find evidence that could “[h]elp
8 defend why we need to ‘protect the graph’” so that Facebook could defensibly deprecate the Events API.
9 However, Chakravarti reported back, after extensive technical analysis, with just the opposite: the Events
10 API comprised a specific collection of endpoints, groups, and permissions in Graph, Rest, and FQL that
11 were being actively used by 5,300 apps on Facebook’s Platform, and “*[t]here doesn’t appear to be any*
12 *illegitimate activity, nor is it concentrated in any single app.*” (PALM-000721698 (*emphasis added*).)

13 178. Facebook nonetheless decided to add the Events API to its Platform scheme. On March
14 24, 2014, Facebook’s Jackie Chang told Simon Cross to deprecate the Events API as part of PS12n and
15 attached an Excel spreadsheet with all the endpoints, groups, permissions, and other functionality the
16 deprecation would encompass. Chang instructed Cross to “include this removal as part of PS12N being
17 introduced at f8” and to deprecate the API on April 30, 2014, along with the Friends and News Feed APIs
18 (PALM-000152576.)

19 179. Facebook used the impending “deprecation” of the Events API to seek reciprocity deals
20 with nearly every major player in the live events / ticketing space. From October 2013 to April 30, 2015,
21 Facebook pursued reciprocity agreements with EventBrite, Ticketmaster, Ticketfly, Fandango, Paciolan,
22 AEG, Flixster, LiveNation, and Stubhub. During this period, Facebook successfully entered into
23 reciprocity agreements with Ticketfly and EventBrite in which Facebook was given access to these
24 developers’ events data in exchange for whitelisted access to Events API functionality.

25 180. On February 28, 2015, Ime Archibong checked in with Simon Cross to ensure that
26 Ticketfly and Eventbrite would be whitelisted for the Events API before the API was publicly deprecated.
27 (PALM-003949478.)
28

FILED UNDER SEAL**E. The Decision to Remove Developer Access to the Friends, News Feed, Events, and Other Crucial APIs Lacked Any Legitimate Justification**

181. The engineers tasked with implementing Zuckerberg’s decision to restrict access to the APIs were baffled. The decision made no technical sense whatsoever. Indeed, there was no justification for it other than to squelch competitors who threatened Facebook’s dominant position and DTBE.

182. As Facebook engineer, David Poll, had written to all Platform Engineers earlier in 2011, the decision would mean gutting the Facebook Platform of functionality used—and needed—by some of the most important mobile apps built on Facebook’s Platform:

I was thinking about the Platform 3.0 friend list change a bit as I was using my Android phone tonight and realized that two for the apps that most impact my day-to-day mobile experience will be completely, irrevocably broken by this change In both of these cases, the apps are adding real value to my experience, and in both of those cases, I have zero expectation that any of my friends will be using the app. The fundamental problem I’m having with this change is that my friend list is my information—it’s part of who I am, and for Facebook to shut down this access primarily comes across to me as FB intruding upon and shutting down my own access to my own information.

183. Poll concluded, “No matter how you slice it, this change is going to have a significant negative impact on my day-to-day smartphone experience.”

184. Poll was correct. The change meant breaking applications that added significant value to Facebook’s network and increased valuable user engagement on Facebook’s core product. The decision to deliberately break these applications had only one plausible purpose—to strengthen the DTBE and to ensure that competitors could not create rival social networks that could compete with Facebook.

185. That proposition was entirely obvious to those responsible for Facebook’s Platform. In an August 2013 e-mail, senior Platform engineer Bryan Klimt wrote to Ilya Sukhar, Facebook’s Head of Developer Products and Senior Engineer working on its APIs, and others working on Facebook’s Platform, stating that the reason for the decision to block access to the Friends and News Feed APIs was to exclude competitors and that all other reasons were simply false and pretextual. To begin with, Klimt was clear that the removal of the APIs was “ridiculous” because they were so essential to the Facebook Platform:

FILED UNDER SEAL

1 I'm trying to write a post about how bad an idea it would be to remove the
2 api that lets you get a list of user's friends from Facebook Platform. In order
3 to illustrate my point, I'd like to satirically suggest removing some API that
4 is so core to the developer experience and that removing it would be
5 ridiculous on its face. For example, removing the Windows API method
6 that lets you create a new window. Or removing the Twilio API method
7 that lets you send a text message. Both suggestions are utterly insane. The
8 problem is, for Facebook Platform, removing the method to let you get a
9 list of friends literally is already that ridiculous. I can't think of an example
10 more ridiculous to parody it with.

11 186. Klimt then dispelled any notion that the APIs were being removed for any technical or
12 functionality-driven reason:

13 Before we discuss in more detail, I'd like to clear up some misconceptions
14 about the deprecations. I've heard some rumors floating around about why
15 we are doing this. But many of them are clearly pabulum designed to make
16 engineers think this decision has solid technical reasons. It does not. 1/ This
17 API can be abused so we can remove it. False. That is a non-sequitur. Lots
18 of APIs can be abused. Our whole product can be abused. That's why we
19 have one of the best teams in the industry at detecting and stemming abuse.
20 That team, plus Unified Review, is more than sufficient to deal with any
21 theoretical abuse coming from this API. Even if this were true, who wants
22 to be in that classroom where the whole class is punished for transgressions
23 of a few?

24 187. Klimt also was clear that the APIs were not being removed in favor of new or different
25 APIs providing the same features:

26 2/ It's okay to remove because we've provided alternatives for common
27 uses. False. If you think that's true, then I don't think you realize why
28 developer platforms exist. If we wanted to limit Facebook to the set of use
cases we've already imagined, we could just do that ourselves, and not even
have a Platform. The purpose of a Platform is to let people build new things
on top of it. It's to enable the whole universe of ideas that anyone in the
world could think of. Developers out there will have all sorts of crazy ideas.
We want them to build those crazy ideas on top of Facebook. Do you know
why Facebook was originally built for the WWW instead of being part of
CompuServe or AOL's proprietary networks? It's because the web is an
open and extensible platform. It lets developers make their craziest become
reality.

188. Klimt then explained that the real reason was to hurt Facebook's competitors and prevent
them from competing with Facebook:

FILED UNDER SEAL

So, if neither of those reasons explains why we are doing this, what's driving it? The only reason I've heard that makes sense is that we are worried about people "stealing the graph", ***we are doing this as a protectionist grab to make sure no one else can make a competing social network by bootstrapping with our social graph.*** Okay, so let's assume for a minute that the social graph does belong to us, and not to our users. And let's even go so far as to assume that this is a real problem, although, I'm not convinced it is. I mean, concerns that other companies will steal our friend graph may just be paranoia. But for the sake of argument, let's say it's not. Then what? ***We're removing the core API in our developer platform. Out of concerns that someone will steal our social network product.*** That sends a clear message to developers: Facebook Platform comes second to Facebook the Social Network Product. This has been a criticism all along with our Platform. When you go read the blog posts critical of our Platform, they all hit on this same point. When our APIs are subjugated to the whims of our other products, they can't be stable. And an unstable platform isn't really a platform at all. So then you are left with 2 big problems. 1/ How do you convince external developers to build on a platform where the most basic core APIs may be removed at any time? I mean, the only big value we bring to the table right now is in distribution and discovery, and that's going to encourage developers to do only the most superficial integration with Facebook. Basically, they're going to do just enough to be able to use Neko ads. 2/ How do you convince internal developers to work on Platform knowing it's only ever going to play second fiddle to the rest of the company? I mean why should any of us work on a product that could be crippled at any time to benefit another team? If I worked on Platform, I would be seriously reconsidering my options if this API gets deprecated.

(emphasis added).

189. Klimt was clear—the decision to remove the APIs lacked any technical or business justification other than to prevent a competitor from creating a competing social network, eroding the DTBE protecting Facebook's business. Any proffered justification by anyone at Facebook to the contrary was entirely pretextual.

190. Moreover, the decision to remove the APIs permanently destroyed the value of Facebook's Platform. If developers could not trust Facebook to maintain the APIs as stable parts of its Platform, they would not risk writing apps for the Platform in the future. The decision meant scuttling Facebook's valuable Platform for the ability to prevent a rival social network from taking hold.

FILED UNDER SEAL

1 191. Sukhar responded to Klimt, noting that he agreed and that he “talks about this every single
2 meeting.” His pleas to Vernal, Purdy and Zuckerberg to reverse their decision fell on deaf ears. The
3 decision had been made and Klimt and Sukhar would have to implement it.

4 192. Facebook continued its audit of apps that relied on the APIs. Most of the Apps were
5 important to the Facebook ecosystem. Indeed, Facebook acknowledged they “are not spammy or crap,
6 but apps users like a lot.” Nonetheless, Facebook’s Papamiltiadis concluded that, among others, apps like
7 Sunrise, Yahoo, IFTT, Friendcaster, MyLife, Sync.me, YouTube, Contacts+, and Bitly “overlap with
8 Facebook products” and “could compromise our success in those areas.”

9 193. Facebook’s careful monitoring of competitive apps continued well into 2013, and given
10 its heavy reliance on data secretly collected by Onavo, Facebook purchased Onavo on October 14, 2013.
11 Facebook used that data to determine which apps competed with its social network and thus posed a threat
12 to the DTBE. It then targeted those companies for withdrawal of API access and coerced data reciprocity
13 agreements.

14 194. In October 2013, Facebook’s Purdy reported that Facebook was dividing apps into “three
15 buckets: existing competitors, possible future competitors, developers that we have alignment with on
16 business model.” Facebook’s Eddie O’Neil believed that the “separation between those categories doesn’t
17 feel clean” and that the overlap was problematic. As O’Neil observed, “apps can transition from aligned
18 to competitive and will ultimately make us sad that we leaked a bunch of data to them when they were
19 aligned.”

20 195. Sukhar objected to the entire exercise, noting that he had been speaking to many dozens
21 of developers “who will get totally fucked by this and it won’t even be for the right reason.” Sukhar
22 explained that his “engineers think *this plan is insane* and I’m not going to support an all hands [meeting]
23 to convince them otherwise.” (emphasis added).

24 196. As Sukhar noted, the decision to withdraw the Friends, News Feed, and Events APIs from
25 the Platform made no technical sense whatsoever, and Sukhar could not bring himself to tell his
26 engineers—who saw through the ruse—otherwise. It was obvious that Facebook was seeking to squelch
27 potential competition—namely, by preventing user growth and engagement for competitive apps. As one
28

FILED UNDER SEAL

Facebook engineer commented about the obvious purpose of the plan to remove the APIs: “I understand we want to make it hard for a developer to grow a new app.”

197. The review of apps continued and specific decisions with respect to certain highly sensitive competitors were escalated to Mark Zuckerberg. As one internal Facebook e-mail explained:

We maintain a small list of strategic competitors that Mark personally reviewed. Apps produced by the companies on the list are subject to a number of restrictions outlined below. Any usage beyond that specified is not permitted without Mark level signoff.

198. In December 2013, Klimt complained to Sukhar about the audit and categorization process:

So we are literally going to group apps into buckets based on how scared we are of them and give them different APIs? How do we ever hope to document this? Put a link at the top of the page that says “Going to be building a messenger app? Click here to filter out the APIs we won’t let you use!”

And what if an app adds a feature that moves them from 2 to 1. Shit just breaks? And messaging app can’t use Facebook login? So the message is, “if you’re going to compete with us at all, make sure you don’t integrate with us at all.”? I am just dumbfounded.

199. As Poll recognized in response to Klimt’s complaint, the changes to Facebook’s Platform were “more than complicated, it’s sort of unethical.” Klimt agreed with the assessment, noting that the API removal “feels unethical somehow It just makes me feel like a bad person.”

F. Facebook Prepares to Announce Removal of the APIs

200. Zuckerberg decided to announce the API removal under the cover of a major change to the Facebook Platform, codenamed PS12N, which would be announced at the next Facebook F8 Developer Conference. Facebook’s engineers were accordingly instructed in September 2013 to bury the changes to the API and announce them quietly along with the changes that would be announced at the conference.

201. In the run-up to its API withdrawal announcement, Facebook continued its audit of applications on its platform that were using the APIs. During that process Facebook continued to classify

FILED UNDER SEAL

1 potential competitors, including LinkedIn and AirBnB, as companies that would be denied access with
2 no whitelist exception.

3 202. Although Facebook knew that the APIs were going to be removed by the next F8
4 conference, it continued to tell developers to rely on them. As a Facebook Platform evangelist noted about
5 one particular document frequently shared with developers, “the language in here around friend
6 permissions is very counter to our upcoming platform simplification efforts” and “feels against the spirit
7 of where we are headed.”

8 203. That was, however, precisely what Facebook wanted—to continue to entice developers to
9 build their software and their businesses on APIs that made them dependent on Facebook. The use of the
10 APIs meant that competitors could be abruptly shut out of the market, useful apps could be extorted for
11 valuable social data, and the rest could simply be destroyed.

12 204. By October 2013, Facebook required certain application developers it chose to whitelist
13 to sign Private Extended API Agreements, which obligated them to purchase large amounts of advertising
14 or to provide their own valuable social data to Facebook in exchange for continued access. That month,
15 for example, Facebook whitelisted Royal Bank of Canada’s application in exchange for the purchase of
16 social data through Facebook’s NEKO advertising platform. Additionally, October 2013 was the month
17 in which Simon Cross and others began actively soliciting Private Extended API Agreements from Events
18 API developers.

19 205. Facebook catalogued and tracked developers on its platform that would likely complain
20 about the decision, creating negative press. Facebook’s internal employees tasked with crafting a PR
21 message explained the undertaking in a December 2013 e-mail:

22 In prep for Platform Simplification, we’re putting together a list of
23 developers who we think could be noisy and negative in press about the
24 changes we’re making: Primarily we think it will be a list of the usual
25 suspects from past policy enforcements. We’d love to pull from your
26 historic knowledge on the topic. Is there anybody you’d add to the list
27 below? We’re going to build plans around how we manage and
28 communicate with each of these developers. There are also comms plans
in the works for working with developers who are high ad spenders and
friends of Mark/Sheryl.”

FILED UNDER SEAL

1 206. Facebook planned to manage its message carefully, as its decision likely would alienate
2 even those developers who were making large purchases of social data from Facebook through ads and/or
3 who were friends of Facebook’s two most senior executives, Zuckerberg and Sandberg. Those developers
4 were identified and the message to them was carefully crafted to avoid a PR disaster. For most application
5 developers, however, the decision would result in the complete exclusion of their applications from
6 Facebook’s ecosystem—which would likely be fatal to their businesses.

7 207. Facebook targeted potentially “noisy” or “negative” developers individually, including,
8 but not limited to, the following applications and developers: iLike, Rock You, Zynga, Path, Flipboard,
9 Slide, Social, Fixer, SocialCam, Viddy, BranchOut, Vince, Voxer, Message Me, Lulu, Anil Dash, Super
10 Cell, Kabam, Washington Post, Guardian, The Wall Street Journal, Jason Calacanis, Cir.cl, Bang with
11 Friends, Tinder, Social Roulette, App Wonder, Ark, Vintage Camera, and Girls Around Me.

12 208. Facebook also used call-log data secretly collected by Android users to target developers
13 and applications to be shut down.

14 209. The entire process led Facebook engineer George Lee to lament:

15 We sold developers a bill of goods around implicit OG [Open Graph] 2
16 years ago and have been telling them ever since that one of the best things
17 they could do is to a/b/ test and optimize the content and creative. Now that
18 we have successes. . . . We’re talking about taking it
19 away [Developers] have invested a lot of time to establish that traffic
20 in our system The more I think about this, the more concern I have
over the pile of asks were [sic] making of our developers this year. PS12N
is going to require them to alter how they deal with APIs (and for limited
value).

21 210. Thus, as Facebook continued to prepare its API withdrawal announcement, Facebook’s
22 own executives recognized that Platform developers had been conned into relying on Facebook’s APIs.
23 Facebook knew full well that it intended to remove the APIs, but it allowed and encouraged developers
24 to build entire businesses on and around them. As Lee put it, they were sold a “bill of goods.”

25 211. By 2014, it was clear that with the exception of a few apps and developers, most would
26 be denied access entirely to the Friends, News Feed, and Events APIs.

FILED UNDER SEAL

1 212. In January 2014, Zuckerberg debated denying API access to dating apps. Facebook
2 decided that it would whitelist Tinder and other anointed dating apps and shut down the rest, clearing the
3 way for the selected apps to dominate the dating market. Zuckerberg reasoned that although Facebook
4 would ultimately create its own dating app, it would let Tinder and a select few others to survive until
5 Facebook's competing app was ready:

6 I've been thinking a lot about Tinder and other people recommendation
7 apps since about 10% of people in many countries are using a Tinder now.
8 People recommendations seems like something that should be right up our
9 alley, but it's currently something we're not very good at. Tinder's growth
10 is especially alarming to me because their product is built completely on
11 Facebook data, and it's much better than anything we've built for
recommendations using the same corpus I think this is a big and
important space and it's something we should have a team working on—
probably to develop people recommendation Hunch sections for now.

12 213. Zuckerberg became increasingly involved in assessing whether individual apps would be
13 whitelisted when the APIs were removed. Facebook's senior-most executives accordingly prepared
14 recommendations for his consideration. In a January 2014 presentation entitled, "Slides for Mark," for
15 example, Facebook employees summarized the results of the ongoing app audit. The presentation
16 observed that the changes would make it "impossible to build" an app without a whitelist agreement with
17 Facebook. The presentation made special recommendations for apps that purchased large amounts of
18 social data through Facebook's NEKO platform or whose developers were friends with Zuckerberg or
19 Sandberg. The bulk of the 41,191 apps that relied on the Friends, News Feed, or Events APIs, however,
20 would be shut out and, as a result, completely destroyed.

21 214. Although the effect on these apps was clear, Facebook continued to evangelize the APIs
22 to developers. In January 2014, Facebook's George Lee sounded the alarm to Purdy and Vernal, which
23 fell on willfully deaf ears:

24 [P]artner managers are still selling products that we ask them to sell, so
25 when it comes to feed integration, we're still telling people to use [Open
26 Graph]. The last f8 was all about implicit [Open Graph], so while we may
27 have decided amongst ourselves that this is no longer the future without an
28 alternative we don't have anything to tell current [developers] (so partners

FILED UNDER SEAL

1 continue to tell them to use [Open Graph] and they continue to integrate
2 it).

3 215. The plan to quietly take away the APIs in favor of a new crippled developer platform was
4 called the “switcharoo plan” by Facebook’s engineers. It was clear to all involved that the announcement
5 of the changes to the platform at the upcoming F8 conference was cover for the radical changes Facebook
6 planned to make to its platform—namely, the removal of the Friends, News Feed, and Events APIs.

7 216. During March 2014, Facebook’s engineers and employees continued to be baffled by the
8 upcoming decision. As one employee noted:

9 It seems a bit odd that we block other developers from doing things on our
10 platform that we’re ok with doing ourselves. Do we consider ourselves
11 exempted? That seems a little unfair especially when our stance on some
12 of these policies is that they’re about ensuring trusts and a great experience.
13 My mental model on how platform is a level playing field could be way off
14 though.

15 217. The decision made no sense to Facebook’s own employees, particularly because Facebook
16 itself needed the APIs to make their own competing applications, including Facebook’s Messenger
17 application. Facebook’s executives ignored all of the concerns raised by their employees, including their
18 API engineers, and continued to drive towards the announcement of the removal of the APIs at F8.

19 218. The real reason for the removal of the APIs was kept tightly under wraps. In April 2014,
20 right before the announcement, Vernal warned Sukhar that if any mention was made of the competitive
21 reasons for the removal of the APIs (as Sukhar wanted), there would be a “high likelihood of breaking
22 into jail.”

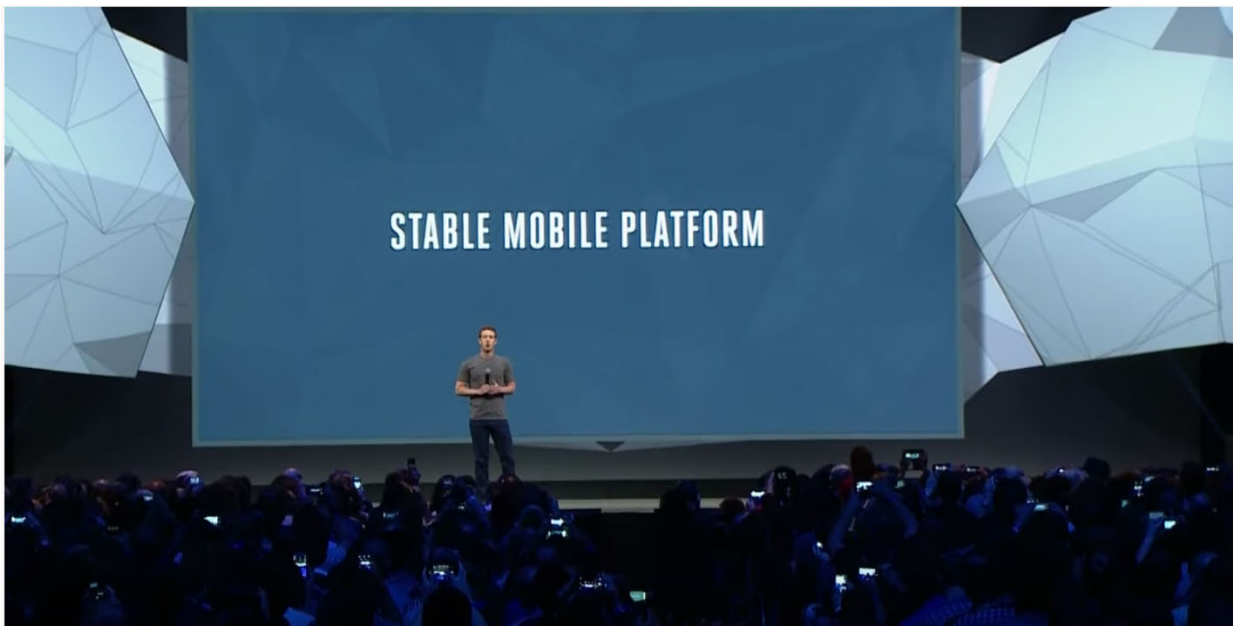
23 **G. The Announcement at F8**

24 219. On April 30, 2014, Facebook announced “The New Facebook Login and Graph API 2.0”
25 on Facebook’s website. Facebook heralded changes to its new Login system for several pages. Buried in
26 the announcement was a quiet statement about the Platform’s most important APIs—the Friend, News
27 Feed, and Events APIs: “In addition to the above, we are removing several rarely used API endpoints;
28 visit our changelog for details.”

FILED UNDER SEAL

220. These APIs were not *rarely used* at all. Tens of thousands of third-party apps were actively using and building on the APIs. Internal Facebook engineers likened them to essential APIs in Microsoft's Windows and were outraged at the removal. Five of the top ten Facebook Apps surveyed in December 2012 relied heavily on them. The announcement was entirely false and was deliberately buried beneath other API announcements to avoid drawing attention to the competition-crippling effect of the decision. In fact, today, the changelog referred to in the announcement is no longer accessible on Facebook's page even though years of other changes are.

221. When Mark Zuckerberg took the stage at F8 days later for his keynote speech, there was no mention of the removed APIs. Instead, Zuckerberg emphasized the "stability" of Facebook's mobile platform just as Facebook quietly removed some of the most heavily relied-upon and necessary APIs in Facebook's Platform.



222. At the twenty developer sessions preceding the announcement, not one mention was made of the API removal or that the upcoming changes would simply break nearly all of the more than 40,000 third-party apps that relied on the APIs.

IV. THE SURVEILLANCE AND ACQUISITION OF COMPETITIVE THREATS

223. To ensure that its scheme to maintain and expand its market power would work, Facebook had to control an important source of competition: independent social networks and producers of social

FILED UNDER SEAL

1 data. Although Facebook could simply destroy any competition that relied on its Platform by denying
2 access to essential APIs, this would do nothing to stop a competitor that was growing its network of
3 engaged users entirely independent of Facebook.

4 224. To detect such threats before they became too formidable, Facebook sought a way to
5 covertly surveil millions of mobile users to determine what applications they were using, and how. Mobile
6 applications were particularly important—and concerning—to Facebook, as desktop engagement was
7 shrinking while mobile apps rapidly proliferated. By 2012, it was clear to Zuckerberg and to Facebook
8 that any threat to its dominance would come from a mobile application. As explained in this section,
9 Facebook used mobile spyware on an unprecedented scale to surveil, identify, and eventually remove
10 from the market through acquisition competitors that independently threatened Facebook’s dominance
11 and/or the DTBE protecting its monopoly, market power and business.

12 **A. Facebook Relies on Onavo’s Surveillance of Facebook’s Competitors, and**
13 **Acquires and Uses Onavo’s Assets**

14 225. Onavo was an Israeli mobile web analytics company founded by Roi Tiger and Guy Rosen
15 in 2010. The company designed spyware designed to surveil users as they used their mobile devices. To
16 obtain extensive information on a user’s usage of mobile applications and of bandwidth, Onavo cloaked
17 its spyware in virtual private networks (“VPNs”), data compression, and even in mobile privacy apps.

18 226. Onavo sold the mobile usage data it collected to Facebook, which in turn used the real-
19 time information it received from Onavo to determine which mobile applications posed a threat to
20 Facebook’s dominance and to the DTBE protecting Facebook from new entrants and competition.
21 Facebook used Onavo data to: (a) identify and target competitors from which Facebook could demand
22 Whitelist and Data Sharing Agreements; (b) identify and target competitors to whom Facebook would
23 completely deny Platform access; and (c) identify and target competitors that Facebook would remove
24 from the competitive landscape entirely through acquisition.

25 227. Facebook received Onavo information in real time, which included the two most important
26 metrics for competing mobile applications—their reach and engagement. Reach measures the size of an
27 application’s user base, and “engagement” measures the extent to which users actively engage with the
28

FILED UNDER SEAL

1 application. An application with high reach but low engagement cannot generate the sort of social data
2 that Facebook needs to feed its advertising platform with actionable targeting data. Conversely, an
3 application with high engagement but low reach doesn't generate social data from enough people to
4 attract a broad base of advertisers. The greatest threat to Facebook's business would come from an
5 application that exhibited strong reach and strong engagement—and especially one that showed rapid
6 growth in both metrics, indicating the development of network effects.

7 228. As the potential threat to its market dominance from mobile applications continued to
8 grow, Facebook sought to obtain exclusive control over Onavo's surveillance data—and over its mobile
9 spyware code and installed base. On October 13, 2013, Facebook acquired Onavo.

10 229. On its blog, Onavo's CEO Guy Rosen and CTO Roi Tiger, announced that Onavo would
11 continue as a standalone brand: "When the transaction closes, we plan to continue running the Onavo
12 mobile utility apps as a standalone brand. As always, we remain committed to the privacy of people who
13 use our application, and that commitment will not change."

14 230. Facebook, however, had other plans. It immediately began integrating Onavo's
15 applications into both its business operations and its acquisition strategy. Facebook, for example, began
16 analyzing data secretly collected from Onavo's Protect software, which was a massive surveillance and
17 data collection scheme disguised as VPN software. Billed as a way to "keep you and your data safe,"
18 Onavo Protect in fact monitored all web and mobile application traffic on a user's mobile device.

19 231. When an Onavo Protect user opened a mobile app or website, Onavo software secretly
20 redirected the traffic to Facebook's servers, where the action was logged in a massive database. Facebook
21 product teams then analyzed the aggregated Onavo data to determine which apps and features people
22 were using in real time, how frequently they used the apps, and for how long. If the data in an app was
23 not encrypted, this information was as specific as (for example) the number of photos the average user
24 likes or posts in a week in that app.

25 232. Based on a 2017 estimate, Onavo's mobile apps were downloaded an estimated twenty-
26 four million times, and Facebook collected, compiled, and leveraged all of the collected data. By February
27 2018, Onavo apps had been downloaded thirty-three million times across both iOS and Android.

FILED UNDER SEAL

1 233. As the former chief technologist for the Federal Trade Commission remarked to the press,
2 Onavo was being leveraged against user interests to stifle competitive innovation:

3 Instead of converting data for the purpose of advertising, they're
4 converting it to competitive intelligence Essentially this approach
5 takes data generated by consumers and uses it in ways that directly hurts
6 their interests—for example, to impede competitive innovation.

7 234. Since 2011 and through the present, Onavo products have provided Facebook with real
8 time data about mobile users on a breadth and scale not available through any other service or app. Using
9 Onavo data, Facebook was able to determine which potential competitors it could target for its Whitelist
10 and Data Sharing agreements; which competitors it could destroy by denying access to crucial APIs; and
11 which competitors is needed to remove from the market through acquisition to preserve its monopoly
12 position and DTBE.

13 235. Moreover, by monitoring potential threats, Facebook ensured that it had no blind spot—
14 any application that posed a threat to its dominance was dealt with through anticompetitive and unlawful
15 Whitelist and Data Sharing Agreements, destruction by denial of access to vital APIs on Facebook's
16 platform, or by acquisition.

17 236. By acquiring Onavo, Facebook obtained exclusive access to the only real-time and high-
18 quality source for mobile app user metrics at scale. Because of the acquisition of Onavo, Facebook
19 strengthened the DTBE by ensuring that any threat to its dominance of the Social Advertising Market
20 was dealt with at the earliest possible stage. Indeed, through Onavo, Facebook was able to (and did) track
21 mobile app usage and trends essentially from launch. If a potential Facebook killer was on the rise,
22 Facebook had a unique tool to identify it before anyone else could—and Facebook used it.

23 237. In the years after it acquired Onavo, Facebook continued to aggressively leverage the
24 company's codebase in deceptively labeled apps that facilitated maximum surveillance and data
25 collection of mobile users. For example, Facebook placed Onavo spyware in apps whose stated purposes
26 required privileged access to user's mobile devices (in some cases, super-user privileges), allowing
27 Facebook to gather data on virtually every aspect of a user's mobile device usage.
28

FILED UNDER SEAL

1 238. The abuses by Facebook were so flagrant that on August 22, 2018, Apple banned
2 Facebook's Onavo app from its App Store. Apple ejected Facebook's app from its marketplace because
3 it violated Apple's rules prohibiting apps from using data in ways far beyond what is required to run the
4 app and provide advertising. In other words, because Onavo Protect was leveraging far more data than
5 any VPN could conceivably need, it was clear that the true purpose of the app was to spy on Onavo users,
6 and Apple would not allow it.

7 239. Indeed, the amount of surveillance was jaw-dropping. Facebook's Onavo Protect app
8 reported on users' activities whether their screens were on or off; whether they used WiFi or cellular data;
9 and even when the VPN was turned off. There was simply no rational relationship between the data
10 collected and the purported purpose of the application. Put simply, a VPN that collected data even when
11 the VPN was off was an obvious subterfuge for blatant spying on user behavior.

12 240. Undeterred, Facebook repackaged its Onavo spyware as a Facebook Research VPN app.
13 Facebook sidestepped the App Store by rewarding teenagers and adults when they downloaded the
14 Research app and gave it root—superuser—access to network traffic on their mobile devices. Facebook
15 has been leveraging its Onavo code in similar ways since at least 2016, administering the program under
16 the codename "Project Atlas"—a name suited to its goal of surveilling app usage on mobile devices in
17 real time.

18 241. When the news broke in January 2019 that Facebook's Research apps were repackaged
19 Onavo apps designed to spy on users, Facebook immediately withdrew the programs from the Apple App
20 store.

21 242. Apple again concluded that Facebook had tried to violate its policies. Using Apple's
22 Enterprise Developer Program, which allows the installation of a certificate or policy that provides root
23 access to an iPhone or iPad, Facebook obtained a level of administrative privilege designed for a
24 company's internal IT department. Thus, using a system that allowed organizations to manage their
25 internal mobile devices, Facebook provided its spyware super user access to regular people's iPhones and
26 iPads. Apple balked at the abuse. An Apple spokesman stated:

FILED UNDER SEAL

1 We designed our Enterprise Developer Program solely for the internal
2 distribution of apps within an organization. Facebook has been using their
3 membership to distribute a data-collecting app to customers, which is a
4 clear breach of their agreement with Apple. Any developer using their
5 enterprise certificates to distribute apps to consumers will have their
6 certificates revoked, which is what we did in this case to protect our users
7 and their data.

8 243. U.S. Senator Mark Warner immediately called for new legislation to prevent the sort of
9 abuse which Facebook had engaged in. U.S. Senator Richard Blumenthal issued a fierce statement
10 rebuking Facebook's repackaging of the Onavo spyware app as "research": "Wiretapping teens is not
11 research, and it should never be permissible."

12 244. In addition to Onavo's Protect app, Facebook has attempted to deploy its surveillance
13 software as other forms of utility applications that require extensive or privileged access to mobile
14 devices. For example, Facebook released the Onavo Bolt app, which locked apps behind a passcode or
15 fingerprint while it covertly surveilled users—and sent Facebook the results. Facebook also shut that app
16 down the very day that its surveillance functionality was discovered. The Onavo Bolt app had been
17 installed approximately 10 million times.

18 245. Facebook continues to possess Onavo's code base and is likely, as it has done before, to
19 repackage its surveillance software into yet another app. Facebook can also easily incorporate
20 surveillance code into any of its mobile applications that enjoy massive installed bases and reach,
21 including Instagram and WhatsApp. If left undeterred, Facebook will likely continue leveraging the
22 surveillance software, infrastructure, and analysis that it acquired as part of its acquisition of Onavo.

23 **B. Facebook Identifies Instagram as a Threat and Acquires the Company**

24 246. Data from Onavo reported a significant threat on the horizon likely as early as 2011 (and
25 certainly by 2012): a photo-sharing mobile application called Instagram. That app had its origins when
26 founder Kevin Systrom, then 27, learned to code over nights and weekends. Systrom developed an app
27 called Burbn, which allowed users to check in, post plans and share photos. The photo sharing feature
28 immediately became the app's most popular.

FILED UNDER SEAL

1 247. After meeting venture capitalists from Baseline Ventures and Andreessen Horowitz,
2 Systrom received \$500,000 of funding. Systrom soon after met co-founder Mike Krieger—then 25 years
3 old—who focused on the user experience of the app.

4 248. Seeing the positive reception to the photo sharing aspect of the Burbn app, Krieger and
5 Systrom decided to pivot their business to focus on that feature. They studied their rivals in the category,
6 including an app called Hipstamatic, which included photo-editing features, including the ability to add
7 filters to photos. Hipstamatic, however, had no social capabilities.

8 249. Seeking to bridge the gap between Hipstamatic photo features and Facebook’s elements,
9 Systrom and Krieger stripped Burbn down to its photo, comment, and like capabilities. They then
10 renamed the app Instagram, containing the words “instant” and “telegram.”

11 250. Systrom and Krieger worked tirelessly to polish the user experience of their new
12 application, designing Instagram to streamline the process of taking photos on mobile devices and
13 uploading them to a social platform. The app had a minimalist focus, requiring as few actions as possible
14 from the user. After eight weeks of fine-tuning, the app entered its beta phase and the founders prepared
15 to launch it on iOS.

16 251. On October 6, 2010, Instagram launched on iOS. That very day it became the top free
17 photo-sharing app on Apple’s App Store, racking up twenty-five thousand downloads. Instagram’s
18 founders were stunned at the response. As Systrom noted after the launch: “First off, we have to say that
19 we never expected the overwhelming response that we’ve seen. We went from literally a handful of users
20 to the #1 free photography app in a matter of hours.”

21 252. By the end of the first week, Instagram had been downloaded 100,000 times, and by mid-
22 December 2010, its total downloads had reached one million. The timing of the app was impeccable, as
23 the iPhone 4, with its improved camera, had launched just a few months earlier in June 2010.

24 253. With Instagram on the rise, investors clamored for a stake. In February 2011, Instagram
25 raised \$7 million in Series A funding from a variety of investors, including Benchmark Capital, which
26 valued the company at around \$25 million. In March 2011, Jack Dorsey, the CEO of Twitter, pursued the
27
28

FILED UNDER SEAL

1 idea of acquiring Instagram, and Twitter made an offer of approximately \$500 million dollars for the
2 company. Systrom declined.

3 254. By March 2012, the app's user base had swelled to 27 million. That April, Instagram was
4 released on Android phones and was downloaded more than one million times in less than one day. At
5 the time, the company was also in talks to receive another \$500 million funding round.

6 255. Internally, Facebook carefully tracked Instagram's meteoric rise, including through the
7 intelligence it received from Onavo's data collection. Instagram clearly posed a competitive threat to
8 Facebook's dominant position, including in the rapidly expanding market for mobile-based social
9 applications.

10 256. Unlike Instagram's streamlined approach to photo sharing, Facebook's photo-sharing was
11 onerous. As Facebook internally recognized, mobile devices were changing how users uploaded and
12 shared photos and it was causing severe problems for Facebook's business. As an internal Facebook
13 presentation explained:

14 Before phones, people would take their digital cameras out for special
15 events, vacations, etc. Then, they would post a bunch of photos at once—
16 after uploading them to their computer. With phones, people take and share
17 more photos more often. They share them individually (rather than waiting
18 to upload a bunch at once).

19 257. This resulted in a large drop in bulk photo uploads on Facebook's core social networking
20 product—a 29% decline from 2012 to 2014. Facebook also observed that text posts were “tanking” 26%
21 because of “migration to phones with cameras.” The data was clear—Facebook had to shut down the
22 looming threat from the new photo-sharing app. If Facebook did nothing, Instagram's user base would
23 imminently eclipse Facebook's at its current growth rate, eroding and perhaps even destroying
24 Facebook's DTBE. An independent app with no ties or reliance on Facebook, Instagram could become
25 not only a competing mobile-based social app, but a social network unto itself that could rival Facebook
26 in the amount of engagement and social data it could produce and monetize.

27 258. In February 2012, Zuckerberg discussed the potential acquisition of Instagram with
28 Facebook Chief Financial Officer, David Ebersman. Zuckerberg explained that he had “been thinking

FILED UNDER SEAL

1 about . . . how much [Facebook] should be willing to pay to acquire mobile app companies like
2 Instagram . . . that are building networks that are competitive with our own.” Mr. Zuckerberg told Mr.
3 Ebersman that these “businesses are nascent but the networks are established, the brands are already
4 meaningful and if they grow to a large scale they could be very disruptive to us.”

5 259. In response, Ebersman asked Zuckerberg whether the goals of the acquisition would be
6 to: (1) neutralize a potential competitor; (2) acquire talent; or (3) integrate Instagram’s product with
7 Facebook’s to improve its service. Zuckerberg replied that the purpose of the transaction would be to
8 neutralize Instagram, saying that the goals of the deal were “a combination of (1) and (3).” He explained:

9 One thing that may make (1) more reasonable here is that there are network
10 effects around social products and a finite number of different social
11 mechanics to invent. Once someone wins at a specific mechanic, it’s
12 difficult for others to supplant them without doing something different. It’s
13 possible someone beats Instagram by building something that is better to
the point that they get network migration, but this is harder as long as
Instagram keeps running as a product.

14 260. Zuckerberg quickly understood that Instagram’s meteoric rise was a threat to Facebook’s
entire business. With a ready-made network of users, Instagram’s dominance of one of the “mechanics”
15 fueling Facebook’s engagement would mean the disruption of the DTBE protecting Facebook. If
16 Instagram took away engagement from Facebook, Facebook would lose some of its ability to target users
17 for content and to advertise to them, which in turn meant less engagement. The virtuous circle would
18 reverse itself.

19 261. As Zuckerberg himself put it:

20 By a combination of (1) and (3), one way of looking at this is that what
21 we’re really buying is time. Even if some new competitor springs [sic] up,
22 buying Instagram, Path, Foursquare, etc [sic] now will give us a year or
23 more to integrate their dynamics before anyone can get close to their scale
again. Within that time, if we incorporate the social mechanics they were
24 using, those new products won’t get much traction since we’ll already have
their mechanics deployed at scale.

25 262. It was clear to Zuckerberg that what he was “really buying is time,” as eventually a
26 competitor would emerge that threatened Facebook’s DTBE and dominance over its walled garden.

FILED UNDER SEAL

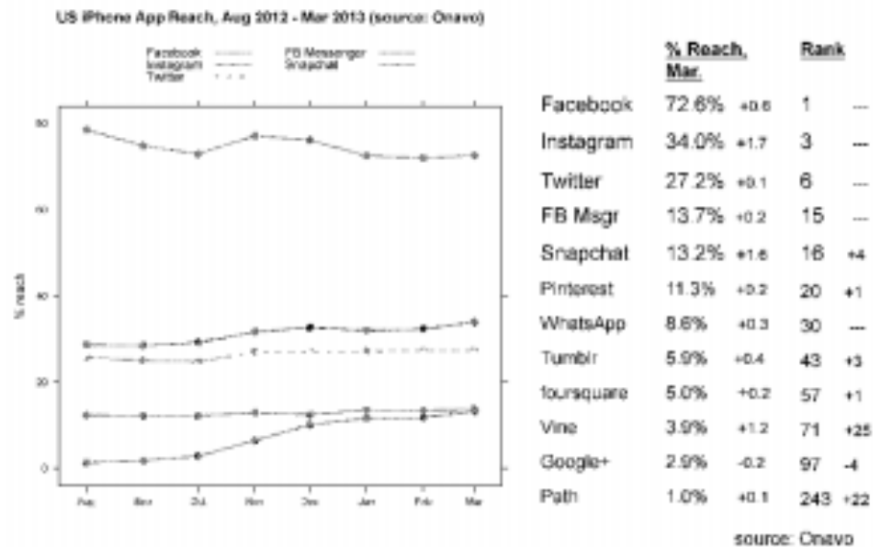
1 Zuckerberg continued the discussion through March 2012, telling Mike Schroepfer, Facebook’s Chief
2 Technology Officer, that acquiring Instagram would provide the company with “[i]nsurance” for
3 Facebook’s main product. Schroepfer agreed, responding that “not losing strategic position in photos is
4 worth a lot of money.” He added that the “biggest risk” would be if Facebook were to “kill” Instagram
5 “by not investing in the company and thereby opening a window for a new entrant.”

6 263. In a message to another Facebook employee on April 5, 2012, Zuckerberg said that
7 “Instagram can hurt us meaningfully without becoming a huge business.” In contrast, he did not view
8 other smaller firms, such as Pinterest and Foursquare, as imminently dangerous competitive threats. As
9 he noted, if these companies “become big we’ll just regret not doing them . . . Or we can buy them then,
10 or build them along the way.” In an all-hands meeting the following day, Mr. Zuckerberg responded to a
11 question about Instagram’s rapid growth by saying that “we need to dig ourselves out of a hole.” He also
12 told employees at the company that Instagram is “growing really quickly” and that it would be “tough to
13 dislodge them.”

14 264. After direct talks with Mark Zuckerberg, Facebook made Instagram an offer to purchase
15 the company for \$1 billion in April 2012, with the express promise that the company would remain
16 independently managed. Facebook consummated the deal immediately prior to its IPO.

FILED UNDER SEAL

265. Facebook's own Onavo data, which was obtained and published by BuzzFeed, made clear that Instagram posed an existential threat to Facebook. By February 2013, Instagram had grown to 34% of the total user reach among all social apps.

US mobile apps (iPhone)

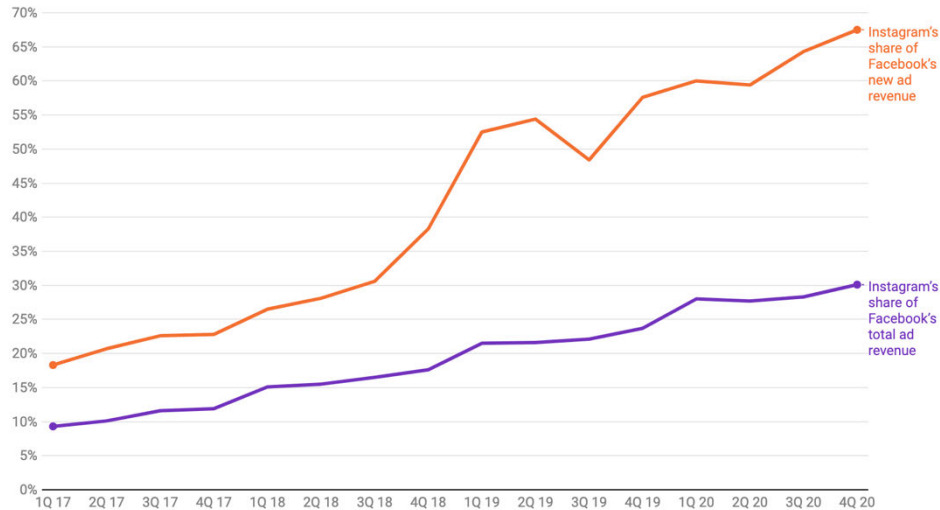
266. With its Instagram acquisition, Facebook's share of mobile photo sharing app users ballooned as Facebook added Instagram's 34% user reach to Facebook's own 72% user reach.

267. Although Instagram had not at the time of the merger meaningfully monetized its user engagement and social data, Facebook quickly did so. By the end of 2013, Facebook had begun showing ads on Instagram. Since then, Instagram has become an ever-increasing proportion of Facebook's advertising revenue and a large share of Facebook's user growth.

FILED UNDER SEAL

268. In 2017, Instagram generated \$2 billion, or about 15 percent, of Facebook's \$13 billion in ad revenue.

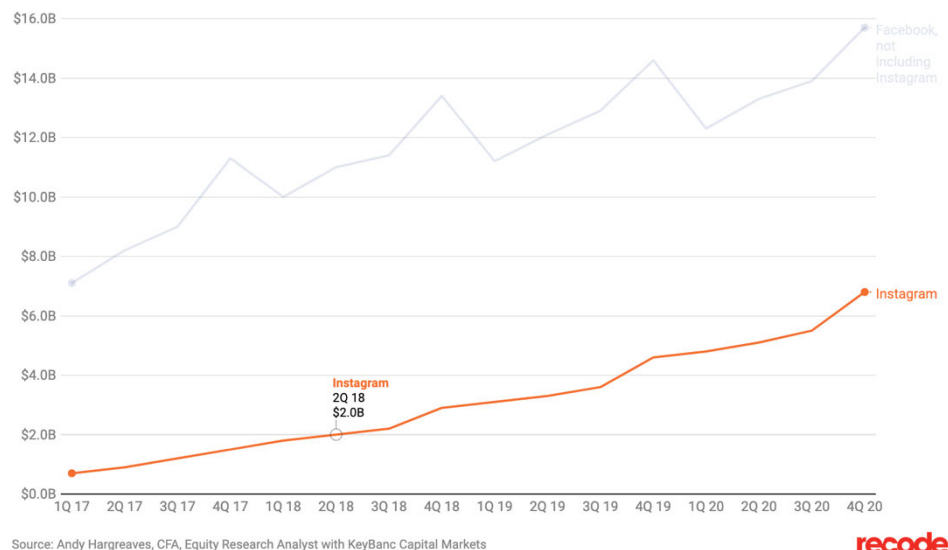
Instagram's estimated share of Facebook's ad revenue and growth



269. By the end of 2018, Instagram had a billion users and was estimated to generate \$8 billion to \$9 billion in revenue for Facebook in 2018.

270. Instagram also accounts for the bulk of Facebook's new revenue since the acquisition.

Facebook and Instagram's estimated quarterly ad revenue



FILED UNDER SEAL

1 271. Instagram allowed Facebook to grow its social network as Facebook’s desktop and core
2 mobile application began to stagnate. Together, Facebook and Instagram captured and monetized the
3 social data generated across both apps.

4 272. The Instagram acquisition ensured that Instagram could not become a rival social network
5 that could generate enough social data to erode the DTBE protecting Facebook’s business. It also ensured
6 that Instagram could not build and grow its own developer platform, which would threaten Facebook’s
7 scheme to dominate the Social Advertising Market by denying and/or leveraging social-data dependent
8 applications’ access to essential functionality. The acquisition accordingly also ensured that Facebook
9 rivals required to enter into Whitelist and Data Sharing Agreements had no other platform choice—and
10 thus no option but to hand over their social data to Facebook. Finally, the acquisition ensured that
11 Instagram could not sell highly targeted advertising in the Social Advertising Market, which would mean
12 there would be a material check on Facebook’s ability to raise prices.

13 273. At the time of its IPO in 2012, Facebook struggled to grow its mobile product, let alone
14 to meaningfully monetize the social data it collected through advertising. By 2019, Facebook had
15 achieved an 83% share of the Social Advertising Market by leveraging its Instagram mobile application
16 and its Facebook mobile and desktop applications. No other company comes close in market share.

17 274. Instagram was instrumental to Facebook’s explosive growth in the Social Advertising
18 Market. From the fourth quarter of 2010 until the first quarter of 2011, Facebook’s revenue was flat.
19 From 2011’s holiday cycle to 2012’s opening three months (right before its IPO), Facebook actually
20 **shrank**. Facebook then experienced a sudden reversal after its acquisition of Instagram, as mobile revenue
21 began to account for a significant share of revenues, and Instagram allowed Facebook to grow with the
22 rise of mobile applications.

23 275. Notably, Facebook’s acquisition of Instagram also allowed Facebook to exclude third-
24 party apps that provided photo and video sharing functionality from its Platform. If an image sharing or
25 video app contained an important feature, Facebook cloned it, thus paving the way for excluding a
26 competitive rival from its Platform, while simultaneously taking away that rival’s share of users.

FILED UNDER SEAL

276. For example, when Snap, the maker of the app SnapChat, rejected Zuckerberg and Facebook's \$3 billion offer to purchase the company and its product, Facebook flagrantly copied key features from Snap and built it into its Instagram product. Thus, when the SnapChat's "stories" feature—which allows a user to post a connected series of images and video—rapidly grew in popularity, Instagram simply cloned it. By late 2016, Instagram had launched a product that mooted one of Snapchat's most popular features.

277. Facebook's own clunky mobile app's clone of the "stories" feature did not have nearly the same traction with users. It was Instagram that provided Facebook the platform to compete head-on with a looming threat among social photo- and video-sharing apps. Without Instagram, Facebook would have faced direct competition. Instead, it leveraged Instagram to obtain and maintain its dominance among social mobile apps and the lucrative social data they generated.

278. Put simply, the acquisition of Instagram dramatically increased Facebook's market share of the Social Advertising Market and strengthened the DTBE protecting Facebook's business.

C. Facebook Acquires WhatsApp

279. In February 2009, Jan Koum and Brian Acton left Yahoo and founded a new company called WhatsApp. Koum had an idea for a mobile application that displayed user statuses in an address book on a smartphone—indicating, for example, whether a user was on a call, had low battery, or was at the gym. The pair enlisted the help of a Russian developer, Igor Solomennikov, to build the app. Koum spent days writing backend code for the app to allow it to sync with any phone number in the world.

280. Although the app—named WhatsApp—was initially unsuccessful, a June 2009 development changed everything. That month, Apple introduced "push notifications" for iPhone, allowing developers to ping app users even when they weren't using the app. Koum immediately updated WhatsApp to ping a user's entire network of friends when their status changed.

281. The feature eventually became a form of instant messaging. Because messages sent through WhatsApp instantaneously notified other users even if the phone was not running the app in the foreground, it became ideal for broadcasting messages to connections within a user's social network, which was built on their phone's contact list.

FILED UNDER SEAL

1 282. At the time, WhatsApp's only significant competition for this sort of instant messaging
2 was BlackBerry's BBM—which was exclusive to BlackBerry's proprietary hardware platform.
3 WhatsApp, on the other hand, tapped into the vast network of app-enabled consumer smartphones that
4 had emerged, particularly Apple's iPhone.

5 283. WhatsApp continued to innovate, including by introducing a double checkmark that
6 showed when a message was read by another user. Wanting more from text messaging, including the
7 limited MMS protocol used by cellular networks, WhatsApp set out to build a multimedia messenger
8 system to send messages across a social network in real time to mobile devices.

9 284. Because WhatsApp's messaging used the mobile phone's Internet connection rather than
10 text messages, the app allowed users to avoid text messaging fees entirely. In some countries, text
11 messages through cellular providers were metered. WhatsApp's ability to send messages to any user with
12 a phone using the Internet was its most sought-after feature.

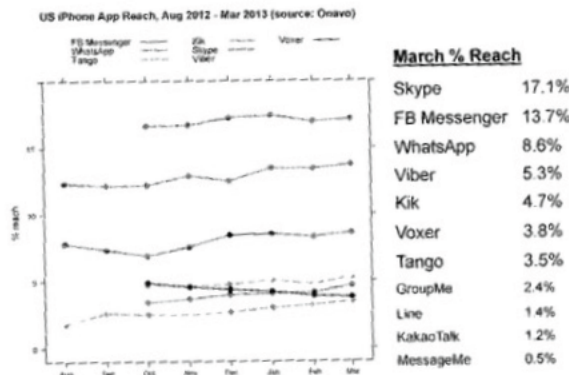
13 285. In December 2009, WhatsApp updated its app for the iPhone to send photos. User growth
14 spiked, even when WhatsApp charged users for its service. Having created a unique combination of image
15 and messaging apps as one socially powered app, WhatsApp decided to stay a paid service and grew
16 while generating revenue.

17 286. By early 2011, WhatsApp was one of the top twenty paid apps in Apple's U.S. App Store.
18 The company attracted the attention of venture capital firm Sequoia, and WhatsApp agreed to take \$8
19 million of additional funding in addition to its original \$250,000 seed funding.

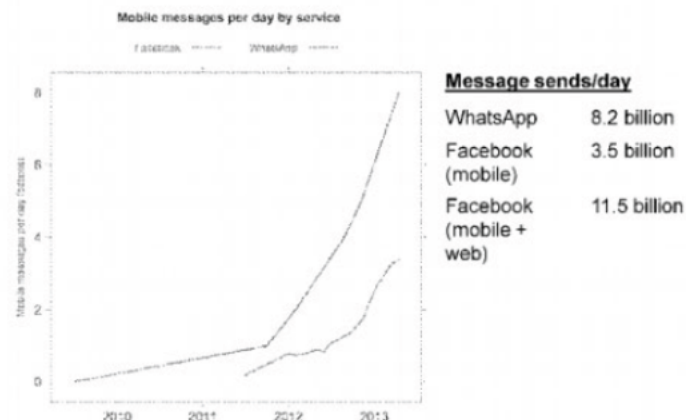
20 287. Two years later, in February 2013, WhatsApp's user base had ballooned to 200 million
21 active users. That month, WhatsApp raised additional funds—another \$50 million from Sequoia, at a
22 valuation of \$1.5 billion.

FILED UNDER SEAL

288. Internally, Facebook had carefully tracked WhatsApp's rapid rise. Engagement data from Facebook's Onavo spyware reported that WhatsApp was rivaling Facebook's own Messenger product and held third place in terms of user reach among mobile messenger apps for iPhone in the U.S as of April 2013.

US mobile messenger apps (iPhone)

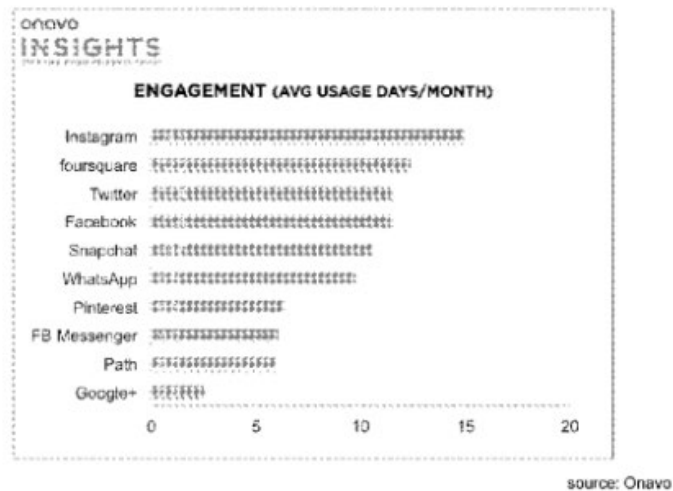
289. The broader picture was even more threatening to Facebook. As BuzzFeed reported, Onavo had tracked messages sent through WhatsApp and the number dwarfed Facebook's own mobile product by more than twofold.

WhatsApp message sends

FILED UNDER SEAL

290. The same Onavo data reported by BuzzFeed showed massive engagement among WhatsApp users, placing it in sixth place behind Facebook's own core product; Facebook's newly acquired Instagram; Twitter; Foursquare; and Snapchat.

US mobile apps (iPhone only)



291. WhatsApp, although lacking Facebook's market reach, was drawing from the same pool of limited attention. Given Facebook's own fledgling Messenger App, WhatsApp exposed a massive vulnerability in Facebook's business model. WhatsApp was built on a social network derived directly from a smartphone user's contact list. It did not require Facebook's graph network for growth and could not therefore be shut down by revoking access to Facebook's APIs. Nor could Facebook demand that WhatsApp enter into a Whitelist and Data Sharing agreement.

292. WhatsApp posed a direct threat to Facebook's business, including the DTBE protecting its dominance. WhatsApp allowed for statuses, image sharing, and texting—all of the principal features of Facebook's core products. By 2013, the size of WhatsApp's network and the user engagement in that network made WhatsApp the most direct threat to Facebook's market dominance—and because of Onavo, Facebook knew it.

293. To ensure that it maintained its DTBE, and thereby its dominance of the Social Advertising Market, Facebook sought to remove WhatsApp as a competitor. As the *Wall Street Journal* reported, Facebook's Vernal internally commented in 2013: "Whats App launching a competing platform is

FILED UNDER SEAL

1 definitely something I’m super-paranoid about.” Vernal understood that if WhatsApp created a rival
2 platform, Facebook’s own scheme to exclude rivals by leveraging its Platform would fail—developers
3 would migrate to the competing platform provided by WhatsApp.

4 294. Internally, Facebook’s management team discussed the WhatsApp threat with urgency.
5 Facebook Director of Growth Javier Olivan wrote in an internal e-mail that WhatsApp had higher levels
6 of reach and usage than Facebook in countries that it had penetrated. For example, based on Facebook’s
7 internal data, WhatsApp reached 99.9% of the smartphone population in Spain, or as Mr. Olivan
8 described it, “literally everyone.” By purchasing WhatsApp, Olivan suggested that they could “grow
9 Facebook even further” by exposing new users to Facebook. Additionally, by bundling free services with
10 WhatsApp and Facebook’s other services, the transaction could serve as another mechanism to expand
11 Facebook’s reach among WhatsApp users. Zuckerberg responded, “I really agree with this analysis.”

12 295. In an email to Facebook’s CFO, David Ebersman, Olivan wrote that WhatsApp’s “reach
13 amongst smartphone users is actually bigger than ours . . . we have close to 100% overlap, our user-base
14 being a subset of theirs.” He explained that “in markets where they do well, they literally reach 100% of
15 smartphone users—which is a big part of the population.”

16 296. On December 13, 2013, Zuckerberg wrote to his management on competitive issues facing
17 the company. WhatsApp was among them:

18 I want to call out two competitive near term issues we face. The first is
19 WhatsApp adding a feature like this for public figures . . . If the space is
20 going to move this direction, being the leader and establishing the brand
21 and network effects matters a lot. This alone should encourage us to
22 consider this soon. . . . When the world shifts like this, being first is how
23 you build a brand and network. We have an opportunity to do this at scale,
24 but that opportunity won’t last forever. I doubt we even have a year before
25 WhatsApp starts moving in this direction.

26 297. Using Onavo data, Facebook’s data scientists modeled WhatsApp’s growth, particularly
27 its engagement and reach, to determine whether it was “killing Facebook messenger,” as well as how its
28 usage trends compared to Snapchat.

FILED UNDER SEAL

298. Knowing about WhatsApp's size, its engagement, and its unique potential to erode the DTBE protecting Facebook market dominance, Facebook moved aggressively to remove this existential threat from the competitive landscape. In late 2013, Facebook made an initial bid of \$16 billion in stock for WhatsApp. During negotiations in early 2014, Facebook raised its price to \$19.6 billion—adding \$3.6 billion to the original price as compensation to WhatsApp employees for staying on board at Facebook. When all was said and done, Facebook ultimately paid close to \$22 billion for WhatsApp.

299. But for the value of containing and shutting down the growth of WhatsApp's competing social network and platform, the transaction made no possible economic sense to Facebook. WhatsApp's revenues were a meager \$10.2 million in 2013. Its six-month revenue for the first half of 2014 totaled \$15.9 million, and the company had incurred a staggering net loss of \$232 million in that same period. Facebook had paid twenty billion dollars—thousands of times WhatsApp's revenues—to acquire a money-losing company that created software functionality Facebook itself already had as part of its own products, and could easily build from scratch for a fraction of the cost of the acquisition if it wanted to.

300. At the time of the WhatsApp acquisition, Facebook's user reach and user base and engagement was already massive—and unrivaled by any competing messaging app—but the addition of WhatsApp's user base further solidified Facebook's dominance in the Social Advertising Market. More importantly, however, Facebook had removed a serious threat to its DTBE. If WhatsApp and its nascent social platform were allowed to compete on the merits, Facebook would not have been able to leverage its Platform into continued dominance of the Social Advertising Market, including by using API access to shut down competing third-party apps and to demanding access to other apps' most valuable social data as a condition for their existence.

301. Moreover, because the reach and engagement on WhatsApp generated (and generates) significant social data that Facebook could (and can) leverage and monetize through its mobile advertising channel, Facebook's DTBE strengthened as a result of the WhatsApp acquisition, fortifying Facebook's unrivaled dominance in the Social Advertising Market, and strengthening Facebook's ability to exclude potential entrants to this market from gaining a foothold with a rival messaging or photo-sharing app.

FILED UNDER SEAL**V. FACEBOOK CONTINUES TO ENTER INTO EXTENDED API AGREEMENTS AFTER THE APRIL 2015 PLATFORM CHANGES.**

302. Facebook continued to enter into Extended API agreements after the April 30, 2015 Platform changes, including in late 2016 and throughout 2017 and 2018.

A. Facebook Continues to Enter Into Whitelist Agreements for Events API Functionality.

303. Many of these new agreements pertained to Facebook's Events API, which allowed developers to publish events to Facebook, view Event Pages on Facebook, and view a list of Facebook Events joined by an application's users and users' friends. Like many core Platform APIs (*e.g.*, those pertaining to friends, news feed, messaging, and media sharing), Facebook's Events API—which comprised a large, enumerated group of endpoints, groups, and permissions—was publicly deprecated in April 2015 as part of Zuckerberg's Platform scheme—despite an engineering analysis of this API concluding that it was widely and actively used (by approximately 5,300 active apps) and that “[t]here doesn't appear to be any illegitimate activity, nor is it concentrated in any single app” with respect to Events API usage. (PALM-000721698, at 699.)

304. This was, however, the point: in early 2013, Facebook made the decision to target advertising based on events-related information, and it had been unable to cheaply acquire sufficient events-related social data to bootstrap this new business on its own. As a result, it had belatedly added the Events API to its PS12N deprecation scheme, and used the upcoming deprecation to solicit reciprocity agreements with targeted events and ticketing companies for their events-related social data.

305. However, as of April 2015, Facebook had not entered into as many of these whitelisting agreements as it had hoped—having reached out to nine of the largest ticketing and events companies in the United States (including Ticketmaster, LiveNation, and AEG), but securing reciprocity agreements with only two events companies—Ticketfly and EventBrite.

306. Facebook's solution was simple: it would simply keep negotiating whitelist agreements for its Events API, which it rebranded as the “Official Events API” in June 2016.

FILED UNDER SEAL

1 307. Between June 2015 and August 2016, Facebook re-upped its extended API agreement
2 with Ticketfly, and entered into new reciprocity agreements with Ticketmaster, Spectra, and TicketWeb.
3 (PALM-003968668.)

4 308. Between January 2017 and July 2017, Facebook entered into at least eight more
5 agreements in which ticketing and events companies granted Facebook “a non-exclusive, transferable,
6 sub-licensable, royalty-free worldwide license to use any Events Data” in exchange for access to the
7 publicly “deprecated” Events API. The whitelisted parties to these agreements included:

- 8 • BigTree Entertainment Private Limited (Jan. 2017)
- 9 • Vendini Ticketing US LLC (Jan. 2017; Apr. 2017)
- 10 • Eventim (Feb. 2017)
- 11 • Songkick (Feb. 2017)
- 12 • SuperBoletos (Apr. 2017)
- 13 • Ticketbox Pte. Ltd. (May 2017)
- 14 • Boletia (Jun. 2017)
- 15 • eTicket (Jul. 2017)

16 309. By May 2017, Facebook required Events API data reciprocity partners to install the
17 Facebook Pixel on their websites and applications as a condition of API access. The Pixel would track
18 ticket sale conversions off-Facebook and transfer that data back to Facebook for use in its ad targeting
19 systems. (PALM-004839673.)

20 310. From July 2017 to May 2019, Facebook entered into at least ten more Events API
21 reciprocity agreements that required events and ticketing companies to grant a full data license to
22 Facebook and to integrate Facebook Pixel on their website and apps in exchange for access to Events
23 API functionality. The whitelisted parties to these agreements included:

- 24 • SeatGeek (Jul. 2019)
- 25 • Eventim (Aug. 2019)
- 26 • Ticketbooth (Sep. 2017)
- 27 • Showpass (Oct. 2017; Dec. 2017)

FILED UNDER SEAL

- ETK BOLETOS SA DE CV (Dec. 2017)
- Eventbrite (Mar. 2018)
- LiveNation (original May 2017; amended Apr. 2018)
- Big Neon (May 2019)
- Xorbia Technologies Inc. d/b/a/ Big Tickets (May 2019)
- Humantix (May 2019)

311. Facebook’s 2017-2019 whitelisting agreements for Events API access—all of which leveraged access to Facebook’s “deprecated” Events API functionality to provide Facebook with event-related social data for use in Facebook’s ad targeting systems—helped Facebook to fortify and maintain the DTBE surrounding its social advertising business. This conduct, which was a continuation of the specific wrongful conduct Facebook engaged in during its PS12N Platform scheme, harmed competition in the Social Advertising Market, and contributed to the anticompetitive overcharge suffered by Plaintiffs and the putative classes.

B. Facebook Continues to Enter Into Whitelist Agreements for Friends API Functionality.

312. Facebook also continued to enter into other Extended API Agreements, including for Friends API functionality, after the April 30, 2015 Platform changes.

313. For example, between May 2015 and November 2015, Facebook entered into at least six Platform API Extension Agreements providing identified developers with access to Friends APIs and other functionality. These developers included Audi (May 2015), Microsoft Windows Phone (June 2015), Sony (July 2015), Harlem App Collective (August 2015), Microsoft Xbox Live (August 2015), and Amazon (November 2015).

314. In August 2016, Facebook entered into an Extended API Addendum with Blizzard Entertainment for access to Friends API functionality.

315. On December 27, 2016, Facebook entered into an Extended API Addendum with NVIDIA that provided NVIDIA with access to Friends API functionality.

FILED UNDER SEAL**VI. FACEBOOK’S NEED FOR “SIGNAL” FROM WITHIN ITS WALLED GARDEN AND ITS EXPANSION INTO NEW SOURCES OF SOCIAL DATA.****A. The Aftermath of the Platform Change and the App Vacuum.**

316. After Zuckerberg made his announcement at F8 in April 2014, Facebook continued to allow access to the Newsfeed and Friends APIs for another year. By the end of April 2015, however, Facebook had finally withdrawn general access to the APIs, destroying tens of thousands of third-party apps on its Platform.

317. Facebook quietly exempted certain developers from its decision, hand-selecting developers from whom Facebook could obtain particularly valuable targeting data; developers that made large ad purchases, especially on Facebook’s new mobile ad platform, NEKO; and developers that met both criteria.

318. Notwithstanding these exemptions, Facebook’s third-party app ecosystem had been decimated. Where thousands of apps previously performed various functions on Facebook’s Platform, allowing Facebook to obtain data from a broad ecosystem of third-party apps for its ad targeting, those apps were now gone—and so was the advertising revenue and user engagement those apps generated.

319. Facebook itself was now the principal (and for many types of user data, only) source of user data from its social network—from within Facebook’s walled garden. Outside developers could, for the most part, no longer query Facebook’s most valuable Graph social data through the Facebook Platform. Rather, Graph data was only available to Facebook and those that it hand-selected for access.

320. Among the apps with high amounts of engagement, Facebook had purchased two of the most successful apps with the fastest growing user bases, WhatsApp and Instagram. Facebook’s core product also included Facebook’s messaging app, Messenger. Facebook’s control over these properties provided it with social data from important social networking vertical products and adjacent features—namely, mobile messaging and photo sharing.

321. With its Platform scuttled, Facebook would have to obtain engagement and social data from its own offerings, but Facebook lacked offerings in major categories, such as travel, e-commerce, streaming video, and location-based services. Facebook could no longer rely on third-party apps to obtain social data from user interactions in those spaces.

FILED UNDER SEAL

1 322. By April 2015, Facebook’s priorities had accordingly shifted. It needed its own direct
2 avenues of collecting user data from within its walled garden.

3 **B. Facebook Relies on User Identity and Engagement to Derive Critical User Intent**
4 **Data.**

5 323. By the middle of 2015, Facebook’s business model was increasingly reliant on machine
6 learning (“ML”) and artificial intelligence (“AI”). Facebook had to collect, structure, and mine social
7 data to derive user intent—information about the user’s intent behind her actions online, including a
8 desire to buy or consume a good or service. To do so, Facebook maintained an “identity”—a profile—
9 associated with each user on its social network.

10 324. Facebook then appended social data collected about the user to a dossier or profile
11 associated with that user’s identity. Facebook’s ability to determine whether a user had a particular
12 interest, was seeking to buy a particular good, or engaged in monetizable activity depended on the ability
13 to first identify the user and then to gather data from the user as she moved through Facebook’s walled
14 garden.

15 325. Facebook’s ML and AI did not take in raw data that was immediately actionable. Facebook
16 had to make predictions about users and needed sophisticated models to do so.

17 326. The predicate task of identifying a user was, for most of Facebook’s existence through
18 2015, trivial. Users logged into the Facebook core product, and anything that user did using that product
19 was carefully monitored and processed as social data. That data was then used to target advertising and
20 content to the user.

21 327. This gave Facebook a significant advertising advantage and a stranglehold over the market
22 it came to dominate—the Social Advertising Market. Facebook was the dominant social network and the
23 gatekeeper for advertising to its users.

24 328. Facebook, however, faced a critical problem after April 2015. It could only mine user data
25 from a limited number of contexts. That was because Facebook’s product offerings, without
26 augmentation from third-party apps, were limited to functions available on the core Facebook product,
27 Instagram, Messenger, and WhatsApp.
28

FILED UNDER SEAL

329. Users, however, were increasingly using the Internet for other functions, such as booking travel; buying and selling goods and other e-commerce; participating in location-based social networking and other location-based services; and streaming video.

330. To ensure that Facebook had enough social data to derive the precious byproduct—user intent—Facebook had to derive rich, mine-able data from as many of these spaces as possible. Internally, Facebook referred to these adjacent, feature-based spaces as “sub-verticals” or “verticals.” Data from these sub-verticals was necessary for Facebook to derive user intent to maintain and fortify its DTBE once Facebook’s third-party app ecosystem was reduced to a handful of chosen players.

331. As Facebook’s Jon Eide, Facebook’s Director and Head of Monetization Applied Research and Strategy, explained in an October 15, 2014, internal Facebook e-mail, “A BIG emphasis on the ads side of the business right now is bringing in these intent signals.” (PALM-006793951.)

332. Facebook was an ad business—first and foremost—but its ad business depended on obtaining social data from users. As a result, once the Platform app ecosystem was crippled by Zuckerberg and his lieutenants’ API scheme, Facebook recognized that it would have to build its own products within its walled garden in order to obtain the “signals”—streams of user data—that it could convert into actionable user intent to maintain the DTBE and its Social Advertising monopoly.

333. Facebook explained signals in an internal presentation, dated Oct. 8, 2018:

1. Signals are measurable events between a user and a business or user events that indicate commercial intent (e.g., search query, etc.).
2. There are three types of signals: onsite (native actions), offsite (pixels, app events) and offline (place-visit-detection, offline API)
3. We leverage the “consumer journey” funnel to map the signal types
4. We will focus this analysis on the value signals provides for ads ranking (vs. ads targeting, organic ranking, etc.)

(PALM-006818179, at slide 2.)

FILED UNDER SEAL**C. Facebook Ventures into E-Commerce to Obtain Signals**

334. Some of the most valuable signals and social data came from observing users make purchases and browse for goods. By the end of 2014, Facebook began developing a product—Marketplace—that would provide users on Facebook with the ability to buy and sell goods, like on Craigslist or eBay. Facebook’s plan was to collect social data as users browsed, posted, and transacted on Facebook Marketplace, then derive user intent information that could be used for precise ad targeting.

335. Such intent signals were also necessary to make product recommendations to users. If, for example, Facebook could determine that a user was looking for a particular type of shoe, it could recommend other similar shoes to the user, increasing the chance that the user would make a Marketplace purchase. This ability was highly monetizable for Facebook, as it provided advertisers on Facebook with a direct means of targeting particular goods to particular individuals who were inclined to buy them.

336. The Marketplace product would, however, directly compete with existing e-commerce offerings, most notably with eBay, a longtime C2C (customer-to-customer) e-commerce giant with close historical ties to Facebook.²

337. Internally, as the destruction of Facebook’s Platform ecosystem loomed in late 2014, Facebook recognized that it would need to derive rich targeting data from various “sub-verticals” to maintain and fortify its social data targeting dominance and the DTBE surrounding Facebook’s business—and e-commerce was one of the most important of these sub-verticals. Without a rich Platform ecosystem of data sources and without the kind of competitive leverage over existing big players that Facebook was able to wield during the Platform scheme, Facebook needed a new strategy to derive social data from key sub-verticals like e-commerce. The company settled upon a new plan: it would actually

² For example, for years eBay had been the parent company of Paypal—a company founded and directed by Peter Thiel, a Facebook board member and close advisor of Mark Zuckerberg. eBay and Facebook also had direct apex-to-apex communications and longstanding business relationships. In 2007, Facebook and eBay collaborated to build an eBay app for the Facebook Platform. (PALM-007694915.) In 2008, Sheryl Sandberg met with eBay CEO John Dohonoe to solicit his help in securing a Facebook-Skype partnership. (PALM-003211348.) In 2010, Dan Rose met with eBay CTO Mark Carges at the Facebook offices to explore “deeper ways that eBay and Facebook can partner together, starting with Facebook connect.” (PALM-006447517.) In 2013, Sheryl Sandberg personally negotiated private advertising purchases on Facebook with eBay. (PALM-003240712.)

FILED UNDER SEAL

1 enter targeted sub-verticals in earnest with Facebook-branded products, thereby capturing needed social
2 data on its own. All that remained was for Facebook to determine exactly which sub-verticals it needed
3 to move into to maintain its DTBE and Social Advertising dominance.

4 338. In order to develop this strategy, Facebook hired more than 100 corporate strategists and
5 put them under Eide, a Ph.D. data scientist who had previously worked at Bain & Company and was
6 tasked with setting Facebook's long-term social data extraction and mining strategy. In particular, Eide
7 and other strategists at Facebook analyzed the company's data targeting business and consumer data
8 trends across the Internet and identified concrete sub-verticals that Facebook should move into.

9 339. Marketplace was one of these—representing a source of rich e-commerce signals that
10 would help Facebook maintain the DTBE, and thereby its Social Advertising market power and price
11 premiums.

12 340. As Facebook delved into the details of its new Marketplace product, its strategists realized
13 that signals would be critical to Marketplace itself, including to develop and optimize the new product's
14 recommendation engine, but also recognized that the flipside was true—signals from a C2C e-commerce
15 product would be invaluable to maintain and protect Facebook's social ad targeting dominance. As Eide
16 explained in his October 15, 2014 e-mail:

17 I bet [signals] could be used for a marketplace optimization (e.g., What
18 types of products to recommend the user). And even the other way around
19 e.g. If we got a large marketplace, we could use their browsing/purchase
history for ad targeting.

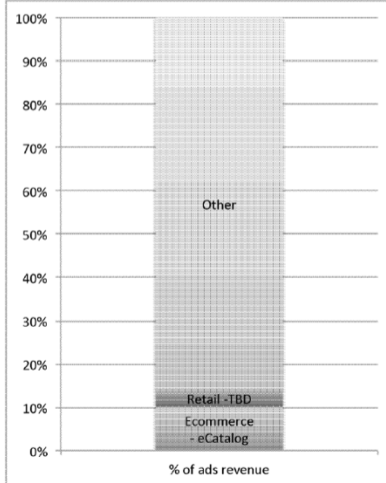
20 (PALM-006793951.)
21
22
23
24
25
26
27
28

FILED UNDER SEAL

341. Facebook's Marketplace product would provide it with important user intent signals, but it would also competitively threaten e-commerce companies that bought ads from Facebook—including eBay. Internally, Facebook flagged the potential conflict:

**eComm-catalog and x-channel mass retail core ads segments
are most at risk from Marketplace (MP) development**

Ads revenue (last 365 days) by sub-vertical at risk



Highest risk sub-verticals are those they share similar marketplace business models:

- **eComm-eCatalog** (~10% of ads revenue or ~\$2B next year) e.g.: Amazon, Wish, Ebay, Zalando, etc.
- **Mass retail with strong online-presence:** (~4% of ads revenue or ~\$800M next year) e.g.: Nordstroms, Walmart, etc.



This is likely an upper-limit and realistic risk will depend on MP approach (next slides)

(PALM-006799270.)

342. As Facebook noted in an internal presentation authored by Eide, dated August 16, 2015, the “[h]ighest risk sub-verticals are those they [sic] share similar marketplace business models,” and those advertisers, including Amazon, Wish, eBay, and Zalando, accounted for approximately \$2 billion of Facebook’s projected ad revenue in the next year. (PALM-006799270.) Moreover, mass retail, such as Nordstrom and Walmart, was expected to spend approximately \$800 million in advertising on Facebook. (*Id.*)

343. One significant source of potential tension between Facebook’s e-commerce advertisers and the nascent Marketplace product was Online Behavioral Advertising (“OBA”) data—data collected from users that respond to third-party ads by clicking or making purchases. Through OBA, retailers and e-Commerce companies that advertised on Facebook handed Facebook actionable data about their customers. With Facebook’s Marketplace product, OBA data from third-party retail/e-commerce activity

FILED UNDER SEAL

1 could be fed by Facebook into its AI/ML models to further strengthen Marketplace against those same
2 third-party retailers/e-commerce sites—and at the same time would concomitantly strengthen Facebook’s
3 Social Advertising dominance through DTBE fortification.

4 344. In 2015 (and thereafter), Facebook collected OBA and other data about its users once they
5 responded to a Facebook ad and went to an advertiser’s site. Facebook continued to track the user (who
6 was uniquely identifiable to Facebook as a specific person in Facebook’s Social Graph, *i.e.*, Facebook’s
7 collection of distinct human persons within its walled garden of apps) on the external site using the
8 Facebook Pixel.

9 345. The name Pixel was given to Facebook’s off-site tracking system because a third-party
10 website embedded a single pixel (a 1x1 image) on pages throughout its site, which would then load from
11 Facebook’s servers as a user traversed the Internet, in many cases triggering cookie reads or writes.
12 Information from the Pixel provided to Facebook a road map of a Facebook user’s off-site activity across
13 the Internet, in real time.

14 346. Facebook’s Pixel allowed Facebook not only to determine whether (and in what way) an
15 identified user responded to an advertisement within Facebook’s walled garden, but to see whether and
16 in what way that advertisement resulted in a “conversion”—a targeted outcome or action, like a purchase
17 or a user’s submission of a form—or some sort of failure. This sort of rich information was fed directly
18 back to Facebook to plug into its AI and ML models, to better target would-be conversions in the future—
19 permitting social targeting by Facebook that could not be replicated by any other would-be Social
20 Advertiser.

21 347. Facebook’s collection of OBA data offsite using Pixel was important to Facebook’s
22 maintenance of its Social Advertising dominance because it made Facebook’s ad targeting more effective,
23 which in turn compelled advertisers to use Facebook’s Pixel on their sites. This created a virtuous circle—
24 as well as a significant conflict with third parties that both competed with Facebook’s Marketplace (and/or
25 other sub-vertical products Facebook introduced after its Platform scheme sunsetted) and advertised on
26 Facebook.

FILED UNDER SEAL

348. Every bit of data these advertisers fed to Facebook, including through the Facebook Pixel, made Facebook's products better—not just its social advertising products, but its new sub-vertical products like Marketplace—which for advertisers like eBay, increased competitive pressure on those advertisers' own products. For Facebook, which cared principally about harvesting data for its ad business, the principal strategic concern was that Facebook needed to fuel its ML and AI systems, and for that, it would need precious signal data, which as the open Platform drew to a close needed to be collected from Facebook's Pixel and from advertisers.

349. Eide, in his August 2015 presentation, succinctly laid out both the feedback loop from Pixel and the potential concerns competitors would likely have:

- Core Ads DR strategy dependent on **optimizing against business outcomes** which requires a signal (pixel, app events, etc.) and optimization against it
- This leads to **prisoner's dilemma** (vicious or virtuous cycle) e.g.,: losing OBA signals (pixel, app events, SPI) → lower performing ads due to less signal → less advertiser sharing signal and optimizing against it, etc.
- Merchants will be worried if FB uses signals to aid competitors and/or FB in the MP, **AND if the merchant doesn't get equal access to that opportunity.**

(PALM-006799270, at 272 (bold text in original).)

350. As Eide observed, convincing advertisers with competing sub-vertical products to provide their data to Facebook for advertising would require assurances that Facebook would treat them equally. This meant that with Facebook's expansion into sub-verticals like Marketplace, competitive and potentially competitive advertisers (e.g., eBay and other e-commerce sites) were hesitant to provide Facebook with Pixel data—a key component of Facebook's data targeting models—unless these advertisers could be assured that they would benefit from the data other similarly-situated advertisers provided to Facebook to train its models.

351. If Facebook played favorites—provided one of its advertisers access to data from other advertisers or allowed large advertisers to opt out of the data pool fueling Facebook's Ad platform—it

FILED UNDER SEAL

1 would undermine the effectiveness of Facebook’s social advertising products, perhaps even triggering a
2 negative feedback loop as Eide noted. This could threaten the DTBE and potentially permit competition
3 at scale with Facebook in the Social Advertising market, thereby killing the golden goose at the heart of
4 Facebook’s entire business: the ability to extract monopoly rents from social advertisers.

5 352. Facebook continued to work on the new Marketplace product throughout 2015 and well
6 into 2016. Facebook internally recognized the risk that the new product posed to its ad revenues—and,
7 through potential negative network effects if large advertisers pulled out of Pixel, to Facebook’s entire
8 Social Advertising dominance. But Facebook needed rich e-commerce signals (and signals from other
9 targeted sub-verticals) after the demise of its Platform in 2015, so simply doing nothing was not an option
10 either. As Mary Ku—a product manager who joined Facebook after a decade at eBay/Paypal—reported
11 to Zuckerberg on August 19, 2015:

12 Impact on ads business: While we are building Marketplace for the long
13 term, if we are not careful, we can have a short term negative impact on the
14 ads business before we build out sustainable value. Several large
15 advertisers are marketplaces and multi-channel retailers who may find our
16 launch threatening to the extent that they may decide to pull ad spend or
17 investment in key strategic ad products (e.g., dynamic product ads). The
18 Facebook marketplace is good for partners who themselves are not
19 marketplaces but clear messaging and value exchange will be needed to
20 help them understand our intentions and value proposition. This situation
21 is particularly risky during Q4 holiday season.

22 (PALM-006214005.)

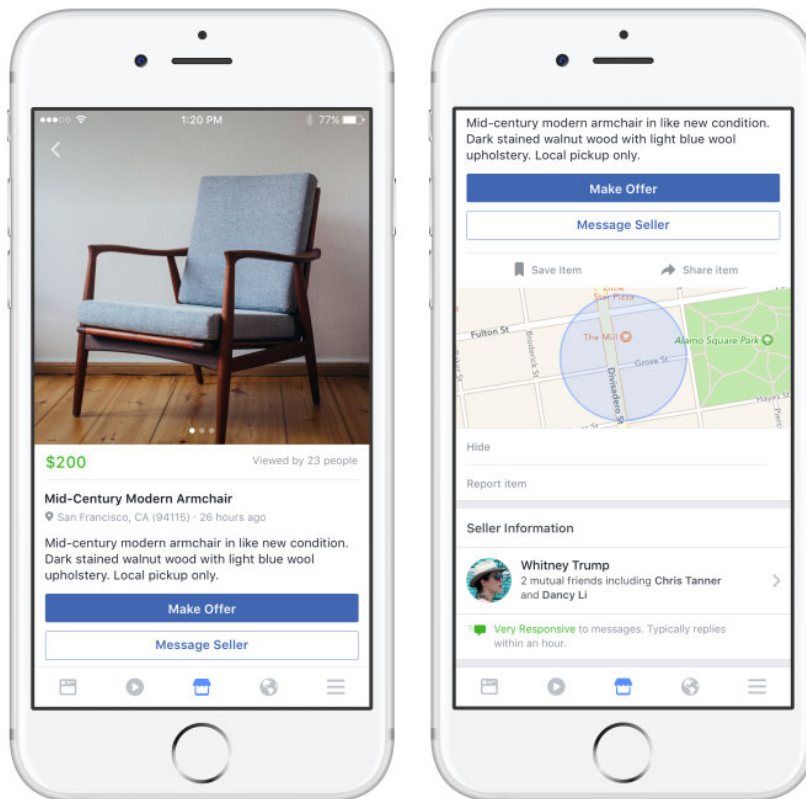
23 353. By January 2016, Facebook quietly rolled out early versions of Marketplace to certain,
24 well-connected users, iteratively testing its product. (PALM-008624396.) The initial results were
25 positive, prompting Facebook to move towards expanding its testing to include additional Facebook
26 users. (*Id.*)

27 354. Facebook launched Marketplace on October 3, 2016, with a focus mostly on customer-to-
28 customer transactions. The initial product was to compete with sites like Craigslist, but Facebook
expected to expand its product to encompass sales from businesses. TechCrunch reported on Marketplace
the same day as its launch, heralding the new functionality:

FILED UNDER SEAL

Facebook Marketplace lets you browse a relevancy-sorted feed of things to buy from people who live nearby, and quickly list your own stuff for sale. Integration with Facebook Messenger lets you haggle or arrange a meet-up, and you know more about who you're dealing with than on anonymous sites like Craigslist thanks to Facebook's profiles.

355. Facebook's Marketplace was launched as the central feature on Facebook's mobile product in 2016. In fact, Facebook placed an icon for Marketplace at the center of its mobile app's navigation bar.



356. TechCrunch noticed the prominence of the new feature. It was clear to the news outlet that Facebook was making a large bet on Marketplace:

Facebook is betting big on Marketplace, considering it's taking over a main spot in the navigation tab bar, replacing the Messenger shortcut in Facebook for iOS. That prime location could make Marketplace the digital version of impulse buys at the checkout counter.

357. Facebook's goal was to rapidly expand Marketplace's exposure to its users. The more Facebook users interacted with Marketplace, the more signals Facebook collected. These signals were

FILED UNDER SEAL

1 some of the most valuable social data Facebook (or any advertiser) could collect: data about its users'
2 intent as they navigated a bazaar of goods.

3 358. What users did in Facebook's Marketplace product (buying, selling, viewing, saving, and
4 *not* buying, among other things) told Facebook's AI and ML not only what identified users wanted to
5 purchase or sell, but also what they were interested in, and how they acted in known potential-purchase
6 situations. Importantly, these signals would come from identified, logged in users, interacting with
7 Facebook's products. Facebook could append the signals and social data it collected to the identity-based
8 profiles powering its ad targeting AI and ML systems—a powerful way to maintain Facebook's DTBE
9 against any would-be Social Advertising entrants.

10 359. On December 18, 2017, then-Facebook Vice President Deborah Liu—another
11 eBay/Paypal alum, who came to Facebook straight from nearly a decade at eBay—and her team internally
12 discussed with Eide the pressure that using signal from a competitive Marketplace product would place
13 on Facebook's ad revenue. "I worry about anti-competitive claims of trying these together as FB
14 marketplace could be seen as a direct competitor to other marketplaces," Facebook monetization principal
15 Robby Banks explained. (PALM-005186374.) A principal focus of the lengthy, multi-email discussion
16 between Liu's team and Eide was eBay. Eide wrote:

17 Imagine E-bay seeing this and realizing that all of their pixel data is now
18 being used to power our marketplace that enables others to compete
19 directly with them with their data. How can we show Ebay that their data
20 is disproportionately helping Ebay? Or any other advertiser determining
21 that we are using their 1st party intent data (e.g. CA inclusion, etc.) in
22 marketplace where they can't compete yet as a B2C? WSJ article will write
23 itself on top of failing our principles.

24 (PALM-005186377.)

25 360. In the first half of 2018, Facebook found auto and rental posts to be the most prominent
26 use cases on Marketplace. (PALM-007676555.) Facebook was harvesting powerful signals from
27 Marketplace, largely because they were based in part on a combination of user behavior, purchases, and
28 searches. This sort of social data was of great value to Facebook's ads business because it showed user
intent.

FILED UNDER SEAL

361. By December 2018, Facebook was testing an extension of its Marketplace product to include full-blown e-commerce features, including purchases while within Facebook's walled garden. Deborah Liu reported on the tests on December 5, 2018:

This past Cyber Week, Marketplace tested extending from C2C to also becoming an e-commerce destination. Even though Black Friday week is an extremely competitive time period, we used this holiday shopping season to build out new user acquisition channels, test messaging to attract new shoppers, improve our understanding of e-commerce, and strengthen merchandising to inform 2019 plans. We exited this week answering a long-term critical strategy question—whether people would trust and be willing to buy products on Facebook at scale. We did 300k transactions in a week which gave us signal that with the right products at the right price, shoppers will overcome trust concerns and buy onsite. More importantly, the platform was stable, having withstood 100+ QPS with a checkout conversion rate of 30%, and now we are closely monitoring post-transaction customer experience with shipping, returns and customer support. It is still really early as we move to e-commerce, but this holiday season proved we can drive onsite transactions and grow this business.

(PALM-002454510.)

362. Facebook carefully monitored the “signals” it was receiving from its Marketplace product. By May 2019, Marketplace was being used a case study throughout the company for onboarding new signals to the company's ad targeting systems. As Facebook's Ashish Nayyar—another eBay/Paypal alumnus, who came to Facebook straight from eight years at eBay/Paypal—reported to Deborah Liu and others on May 17, 2019:

Case study: lastly, Marketplace is being used a [sic] case study across the company to onboard other surfaces into the broader signals xfn to use organic signals across ig, blue, messenger and wa.

(PALM-010596356.)

363. Marketplace signals also drove revenue from Facebook's News Feed. As an October 24, 2018, report from Brad Winters to Deborah Liu stated:

Marketplace Signals in News Feed Ranking: We currently estimate MP signals drives +0.5% incremental News Feed revenue, and estimate it will grow to +0.75% by Q4'19. Based on conversations with the DS team, we

FILED UNDER SEAL

believe this is a lower bound and the ads signals team is running tests this quarter to refine this estimate.

(PALM-003883413.)

364. Facebook had successfully moved into the e-commerce space, pitting its business against the likes of Craigslist and eBay. However, as explained in Section VI of this Complaint, instead of simply competing on the merits in this new sub-vertical, Facebook leveraged its entry into the space to strike a series of anticompetitive deals with its longtime business partner eBay that would provide Facebook with the data and signals it needed to maintain its Social Advertising monopoly without the burden of aggressive competition with e-commerce rivals. Facebook's agreement with eBay helped to fortify Facebook's DTBE and maintain its monopoly position in Social Advertising, at the expense of competition in e-commerce sub-verticals—and to the detriment of Social Advertising consumers like the Plaintiffs and the putative classes.

D. Facebook Moves into Location-Based Services

365. By the end of 2015, Facebook faced nascent competition from a growing location-based social network, Foursquare. Foursquare had expanded the concept of the social network to the physical world, allowing its users to “check in” at various locations, notifying friends of their whereabouts.

366. In July 2014, Foursquare had split itself into two apps—Swarm and Foursquare. Swarm would focus on location-based messaging, while the Foursquare app would focus on local recommendations based on a user's location. Both apps threatened to make inroads on Facebook's social networking business through innovations in location-based services.

367. Foursquare had laboriously developed the data required for its location-based social network, including information about places of interest, restaurants, shops, and other places frequented by its users. Foursquare provided this information to third-party integrators and apps through the Foursquare API. TechCrunch described Foursquare's data, API, and network of integrators in a May 5, 2015, article:

Places by Foursquare, meanwhile, is the company's repository of Places, a database of about 65 million points of interest that the company says can be used as an end-to-end location solution. This is the database that is built

FILED UNDER SEAL

1 out not just through the network of developers who use Foursquare's
2 API—which includes companies like Citymaps, Microsoft and Garmin—
but also through Foursquare's own apps.

3 368. Foursquare's database of Places gave it a running start against Facebook in the rapidly-
4 developing location-based services sub-vertical, and the company had aggressively built a competing
5 social network using that head start. In December 2015, Foursquare raised an additional round of funding
6 based on the premise that the data it had gathered was uniquely valuable.

7 369. But worse for Facebook than simply Foursquare's nascent social network was the
8 company's rich trove and pipeline of real-time socialized location data. Such data—which could
9 potentially be used to powerfully target social advertisements in the right hands—was imminently
10 licensable from Foursquare through its API, and this posed a significant potential threat to Facebook's
11 Social Advertising monopoly. If Foursquare's real-time location data repository and pipeline were
12 provided to a potential entrant at scale in Social Advertising—or Foursquare itself grew its Social
13 Advertising products with a valuable location-based data trove while Facebook was itself still preparing
14 for meaningful entry into location-based services, this could significantly erode the DTBE, as location-
15 based targeting and inferences and signals relating to location were on the verge of becoming perhaps the
16 most valuable targeting signals for social advertising.

17 370. Unfortunately, Foursquare was at least a year ahead on location-based data—and the
18 company's expansion into social networking in earnest threatened to marry location-based services with
19 targeted social ads, imperiling Facebook's Social Advertising monopoly.

20 371. As with so many other critical competitive decisions in the months and years after the
21 2015 demise of the open Platform, Facebook's response was to announce its own product in the location-
22 based services sub-vertical, then seek to cut an anticompetitive deal with a leading competitor in that sub-
23 vertical. In location-based services, Facebook sought out Foursquare, and cut a deal to maintain its Social
24 Advertising monopoly at the expense of its new sub-vertical product.

25 372. As for Facebook's new product in the location-based services subvertical, that answer
26 came (publicly) in the first half of 2017. Specifically, by the end of March of 2017, Facebook was
27 preparing to launch a new product—the Places Graph. This product was an API designed to allow
28

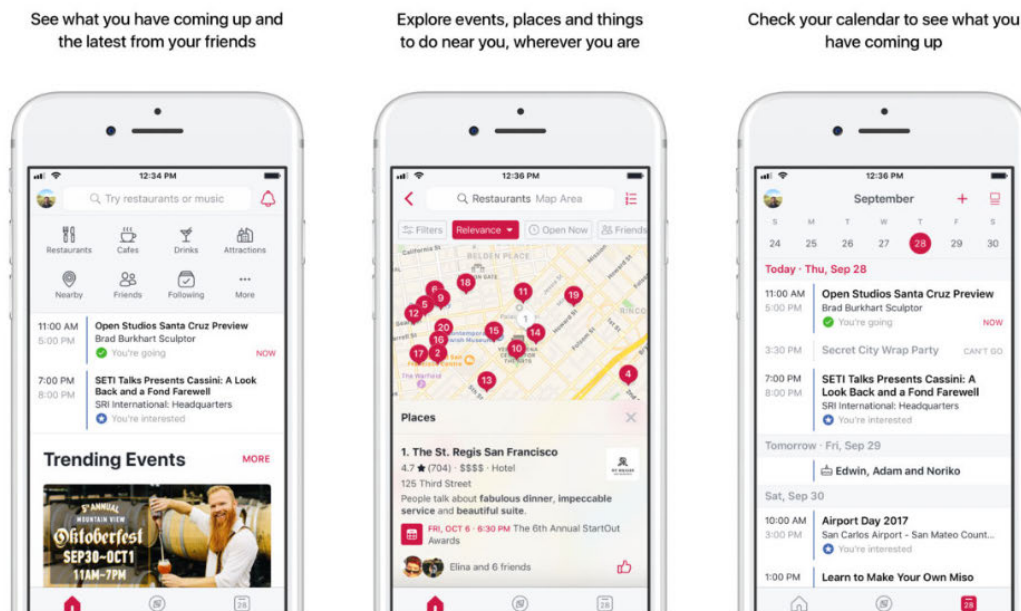
FILED UNDER SEAL

advertisers to target customers and content by location, providing a direct competitor and replacement for Foursquare's rival location-based APIs. Its first incarnation of Facebook's Places Graph accomplished this by providing information about points of interest necessary for check-in and photo geo-tagging functionality. Facebook's Anthony D'Souza described the launch version of the Places API product in a March 10, 2017 e-mail:

For context, this is a new API we are launching that will give third-party developers access to information about 140M+ points of interest around the world (e.g., place name, opening hours etc.). It's the data set that powers use cases such as geo-tagging on Facebook and Instagram and live location sharing on Messenger.

(PALM-003853378.)

373. Facebook planned to leverage this new technology to create a "Local" app or feature that would allow Facebook to target advertising by location. (PALM-007188391.) Facebook launched the app on November 10, 2017. The new app provided a feed providing information about friends' locations and nearby places of interest.



FILED UNDER SEAL

374. Internally, Facebook projected that it would acquire significant daily user interactions from the launch of its Local product—one that would rival TripAdvisor, Yelp, and Foursquare. Facebook’s Aditya Koolwal provided the projection in a January 24, 2018 e-mail:

Question 1: How many people do we expect to use the Local app (in the long run)?

We are approaching this in two ways:

1. Lower bound: Assume that some percentage of Local Intentful DAP on Facebook will use the app (based on Events penetration in that country)

2. Upper bound: Assume that we can be better than competitors (TripAdvisor, Yelp, Foursquare) in markets where we have reasonable traction with Events (Europe, North America, Latin America).

Preliminary numbers suggest a potential DAP in the 10-20M range, which is in line with previous estimates. If we assume that we can achieve excellent performance in APAC, our long-term potential DAP increases to ~30M.

(PALM-007374711 (bold text in original).)

375. Notably, Facebook leveraged Onavo spyware data (described below) to determine where its new product would fit among the competition:

We are also looking at apps more generally to see which ones exceed 100M DAP. In the Local space, only one app clears that bar: Google Maps (216M). Other mapping products are surprisingly smaller (Waze: 23.3M DAP, and Apple Maps: 7.03M DAP) based on Onavo data.

(*Id.*)

376. Facebook planned to collect valuable social data from its new Local app—namely, information about its users’ interests, whereabouts, and interactions among connected Facebook friends. This data provided much needed signal within Facebook’s walled garden. Local was another property Facebook could use to collect social data that Facebook’s AI and machine learning systems could convert into user intent data as well as other data that would strengthen Facebook’s social ad targeting.

377. If Facebook could build its own location database and app—as it was planning to do in 2017—it was positioned to compete against Foursquare and other location-based apps, such as Yelp. As

FILED UNDER SEAL

1 explained in Section VI of this Complaint, however, Facebook did not end up competing on the merits
2 with Foursquare. Instead, Facebook entered into an anticompetitive agreement with FourSquare to end
3 competition between the two companies—permanently.

4 378. In 2018, faced with a threat to its Social Advertising monopoly from Foursquare’s
5 location-based data trove and pipeline, Facebook used its imminent entry into Foursquare’s sub-vertical
6 to cut a data deal with Foursquare that helped to fortify Facebook’s DTBE and maintain its monopoly
7 position in Social Advertising, at the expense of competition in the location subvertical—and to the
8 detriment of Social Advertising consumers, including Plaintiffs and the putative classes.

9 **E. Streaming Video and Facebook Watch**

10 379. Another potential source of user social data that could be mined for ad-powering targeting
11 information was streaming video. By 2016, Facebook had included a video tab in its mobile product, but
12 long-form and episodic videos were taking hold in the market—and formed a particularly rich source of
13 potential social data targeting.

14 380. In 2017, Netflix was the pre-eminent streaming service that specialized in long-form
15 television and movie content. Netflix’s streaming service had grown significantly, from approximately
16 \$8.8 billion in revenue in 2016 to \$11.6 billion in revenue in 2017.

17 381. Netflix was also a powerful source of user data. The movies, TV shows, clips, sports, and
18 episodic videos its users watched and interacted with shed light on their interests, as well as their likely
19 purchasing decisions.

20 382. At the heart of Netflix’s service was its recommendation algorithms. Netflix’s
21 recommendation algorithm tailored content to particular users. As the Wall Street Journal explained in a
22 November 10, 2018 article: “Analytics is deeply embedded in Netflix’s DNA. The company mines reams
23 of data on its subscribers’ tastes to help determine which shows to bet on and how to promote them.”
24 Moreover, Netflix uses powerful AI and ML models to determine which shows and movies to license
25 and what original programming to create.

26 383. After the demise of Platform, Facebook knew it needed a rich source of video interaction
27 data for its AI and ML models in order to maintain the DTBE protecting its Social Advertising monopoly.
28

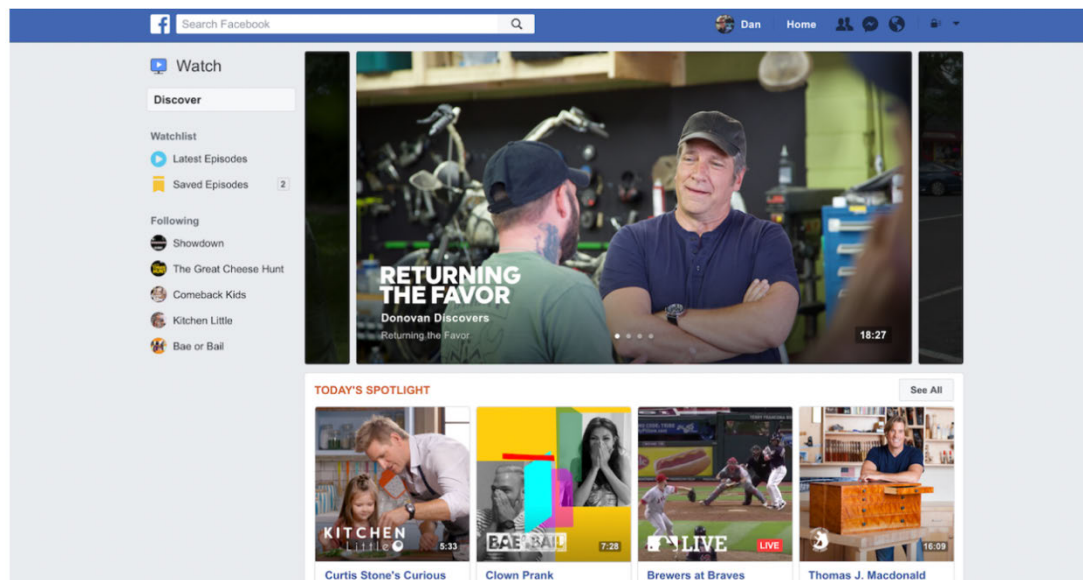
FILED UNDER SEAL

Too many users were spending too much time watching streaming video—especially algorithmically-recommended long form videos, which generate especially powerful signal information about user’s interests and attention—for this to be a blind spot in Facebook’s ad targeting models. Absent such a data source for Facebook’s models, a potential Social Advertising entrant—or perhaps an existing Social Advertising participant—with access to rich long-form video interaction data could erode, or perhaps even surmount, the DTBE surrounding Facebook’s social advertising business, and threaten Facebook’s supracompetitive profits.

384. Moreover, a video offering was needed to increase users’ session times on Facebook. If Facebook could keep its users within its walled garden, it could readily identify them, track them, and advertise to them.

385. Facebook’s response to this was twofold: to seek out a data deal with a rich source of video interaction data, and to directly enter the long-form video market at scale with Facebook’s own streaming video offering.

386. On August 9, 2017, Facebook introduced its own streaming video product, called Watch. The new product appeared as a tab on the Facebook homepage and mobile app.



FILED UNDER SEAL

1 387. Facebook monetized Watch directly by keeping a portion of video ad revenue, but Watch's
2 true value was the rich data Facebook would collect, mine, and feed into its AI and ML systems from
3 users' engagement and interaction with Watch.

4 388. Watch allowed video to be tailored to individual users, including based on their network
5 of friends and their habits. Facebook also curated video to users based on what others on its network were
6 watching. As TechCrunch explained in an article dated the same day as Watch's launch:

7 Watch features personalized recommendations of live and recorded shows
8 to watch, plus categories like "Most Talked About," "What's Making
9 People Laugh" and "Shows Your Friends Are Watching." Publishers can
10 also share their shows to the News Feed to help people discover them. A
11 Watchlist feature lets you subscribe to updates on new episodes of your
12 favorite shows. Fans can connect with each other and creators through a
13 new feature that links shows to Groups.

14 389. Watch entrenched the user on Facebook's social network. The purpose was to integrate
15 video with the rest of its product, and to increase the time Facebook's users spent on Facebook
16 properties—inside Facebook's walled garden.

17 390. Increased watch time for videos also meant that it was more valuable to advertise on
18 Facebook's video platform. As Facebook's Kelly MacLean noted in an internal Facebook e-mail setting
19 out talking points for Brad Smallwood, dated July 23, 2017: "As video takes off and becomes a higher %
20 of ad spend on our platform, duration and watch time are becoming increasingly important for many of
21 our clients." (PALM-007979632.)
22
23
24
25
26
27
28

FILED UNDER SEAL

391. In January 2018, Facebook began internally compiling watch-time data as well as common queries for various categories of videos. Among the various categories, TV shows, funny videos, news, and sports resulted in millions of minutes of watch time:

Potential Video Intent Queries

Type	Queries	Volume (Daily)	WT (Mins)	Retention	Top Countries (Vol)	Top Countries (WT)
FB Shows	ball in the family	115K	500K	tbd	US, PH, IN	US, PH, CA
TV Shows	enamorandonos	7.5M	18.8M	tbd	PH, US, MX	PH, MX, MY
Movies	coco	4.4M	6.1M	tbd	PH, US, MX	PH, MX, MY
Music	ozuna criminal	2.1M	2.3M	tbd	PH, US, MX	PH, MX, US
Categorical	funny videos	8.3M	12.7M	tbd	MX, PH, ID	MX, PH, PE
Publishers	tasty	2.0M	1.6M	tbd	IN, US, PH	US, PH, IN
Creators	xander ford	2.5M	3.75M	tbd	PH, US, IN	PH, US, MX
Food / Recipes	chocolate cake	2.3M	1.0M	tbd	US, IN, PH	US, PH, IN
News	pistorius sentence increase	27.0M	11.5M	tbd	US, PH, IN	US, PH, MX
Sports	barcelona live	3.5M	7.1M	tbd	MX, PH, US	MX, PH, US
Gaming	minecraft	1.3M	570K	tbd	US, PH, BR	PH, US, MY
Beauty / How To	smokey eyes makeup	1.0M	315K	tbd	US, PH, GB	US, MY, FR

(PALM-005529364.)

392. However, as with Marketplace and Local, Facebook's entry into streaming video posed a threat to the advertisers on its ad platform that also had streaming video services, including streaming giant Netflix—whose founder and CEO Reed Hastings was a member of Facebook's Board of Directors.

393. As explained in Section VI of this Complaint, Facebook again leveraged its entry into a sub-vertical—here, video—to cut an anticompetitive deal with a would-be competitor to maintain its Social Advertising monopoly. In particular, Facebook entered into a series of deals with Netflix—headed by Facebook's own board member—to cripple competitive aspects of the Facebook Watch product in exchange for Netflix data that could supercharge Facebook's ad-targeting systems and maintain the DTBE and Facebook's Social Advertising monopoly. This injured Social Advertising consumers, including Plaintiffs and the putative classes.

FILED UNDER SEAL**VII. FACEBOOK’S ENTRY AND DATA CAPTURE CONDUCT****A. Facebook Enters Markets to Leverage Agreements that Maintain and Fortify Its Social Advertising Monopoly**

394. Facebook’s business has long relied on selling advertising targeting users that interact with its properties, including Instagram, WhatsApp, Messenger, and its core Facebook product. As users actually interact with these products—*e.g.*, a user browses Instagram; chats via WhatsApp or Messenger; or navigates Facebook’s website or mobile app—their identities are readily ascertainable by Facebook. These users are logged in to Facebook, and their every move tracked, logged, and converted into structured social data to be mined by Facebook’s ML and AI systems.

395. By 2015, Facebook’s users were using smartphones and web applications to perform time- and attention-consuming activities that Facebook had not made part of its owned-and-controlled product. Worse still, after the (pre-planned) demise of Facebook’s open Platform in early 2015, Facebook’s network of external sources of social data—the sorts of “signal”-rich activities that helped Facebook target social advertisements, and would help it build ML / AI models to even more accurately target social advertisements in the future, thereby maintaining the DTBE protecting Facebook’s Social Advertising dominance—was crippled.

396. As a result, by 2015 Facebook again faced an existential dilemma for its Social Advertising monopoly: Facebook lacked signal-rich data from particular types of online activities (*e.g.*, e-commerce; location-based services; longform streaming video) to build out its ad targeting models, and a failure to obtain such data in the near-term risked eroding the DTBE to a point where a serious competitor could enter the Social Advertising Market and check Facebook’s supracompetitive ad prices.

397. Facebook could not risk any major blind spots in its valuable “signal” of social data, or else it could not effectively track identity outside of its properties. This would lead to a negative feedback loop: poor signal meant advertisers would not be attracted to advertising on Facebook because Facebook’s targeting would be inferior, and because Facebook mined the information it gleaned from advertisers and their advertisements, Facebook would lose more valuable signal to mine for its ad targeting, making its ad products even less attractive to advertisers. In short, Facebook’s ability to access

FILED UNDER SEAL

1 these newly ascendant data sources meant the difference between a monopoly-maintaining virtuous circle
2 (the DTBE)—and a death spiral in the Social Advertising Market.

3 398. Facebook recognized it had two options to obtain the data it vitally needed to maintain
4 and enhance its market power: it could personally enter markets that generated such data (Facebook called
5 them “sub-verticals”), introducing new products at scale in e-commerce, location-based services,
6 longform streaming video, and the like; or it could get the data from existing market leaders in those sub-
7 verticals.

8 399. As to the latter option, Facebook had been trying for years to get rich targeting data from
9 other major Internet companies—this was one *raison d’etre* of its earlier Platform scheme—but after
10 2015, Facebook’s leverage dried up against companies like eBay, Netflix, and Foursquare, all giant data
11 sources that could potentially service Facebook’s monopoly maintenance needs, but which as of 2015
12 were resistant to Facebook’s entreaties.

13 400. As a result, Facebook settled upon the former option—introducing directly competitive
14 products in key sub-verticals, including e-commerce, location-based services, and longform video. Thus,
15 between 2016 and 2018, Facebook made plans to introduce Facebook Marketplace, the Facebook Places
16 API, and Facebook Watch.

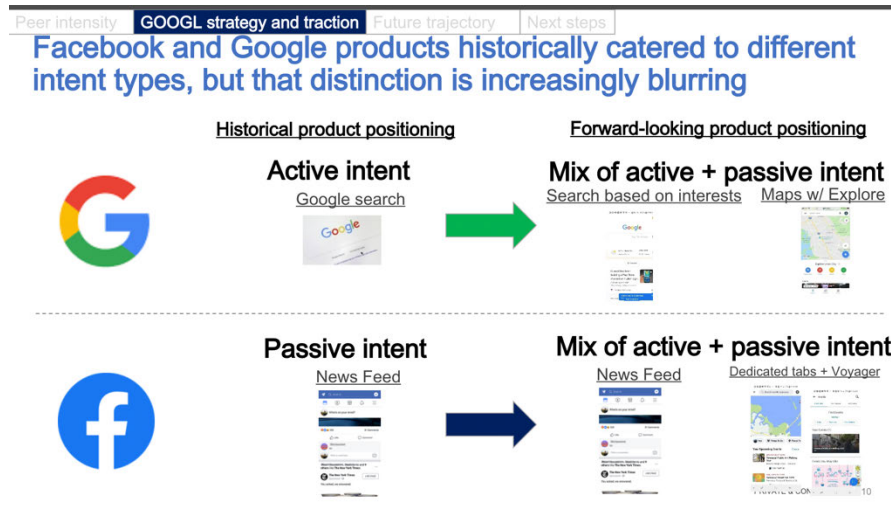
17 401. Indeed, from 2016 through the present, Facebook aggressively entered sub-verticals that
18 contained valuable signal that Facebook could mine for actionable user intent data. It was this user intent
19 data that advertisers found attractive.

20 402. Facebook needed this data for its social advertising business because of its AI and ML
21 models. Unlike search giant Google, which had data that directly evinced its users’ intent, Facebook had
22 to determine user intent indirectly from its users’ behavior.

23 403. Facebook’s AI and ML systems were designed to infer user intent from “passive”
24 signals—such as behavior characteristics associated with a particular user or from distinct user attributes
25 and social interactions.

FILED UNDER SEAL

404. A search engine, such as Google's, receives a stronger indication of a user's intent, as the user enters what she is looking for into a search bar. As Facebook recognized in a June 2019 internal presentation, its method of monitoring user behavior and interaction with Facebook features, such as the Facebook newsfeed, was a passive form of user intent. Making inferences that translated passive, behavioral signals to actionable user intent required more sophisticated models.



(PALM-008492596, at 606.)

405. Moreover, Facebook needed what it called "identity" to make inferences about its users' intent. This was because Facebook needed a collection of a user's data to identify attributes that are predictive of their intent. An internal 2015 Facebook presentation defined identity, as used in the digital advertising context, along these lines:

Identity is "the collection of identifiers and traits of a single person across devices and browsers to support advertising decisions and measurement[.]"

(PALM-011711092, at 098.)

406. In other words, a key to making user intent predictions is the ability to ascertain a user's identity, then to associate the data collected (sometimes across devices) to that user, before feeding the user's profile into ML and AI systems.

407. For Facebook, it is trivial to identify users within its own walled garden. After all, these users are logged into Facebook. Outside of its properties, however, Facebook must probabilistically ascertain the identity of a user, then match the identified user with her Facebook-maintained profile. In

FILED UNDER SEAL

1 other words, outside of Facebook's walled garden, advertisers such as Google have better insight into
2 tracking individuals across the internet, including across websites.

3 408. Facebook's goal was therefore twofold: (a) to collect social data that it can mine for user
4 intent; and (b) to do it while the user is within its walled garden and easily identifiable.

5 409. Facebook's subvertical strategy was in pursuit of these goals. By 2015, Facebook knew
6 that it needed (or would soon need) for its advertising models rich data from users' e-commerce
7 interactions; from location-based check-ins and movements; and from the increasing hours of active
8 video-watching as longform, premium video content moved online with Over-the-Top (OTT) streaming.
9 This was a competitive necessity going forward—especially for a monopolist in a network effect-based
10 market. Moreover, by providing location-based services, an e-commerce platform, or longform streaming
11 video, Facebook would increase the amount of time its users stayed on Facebook. For example, if users
12 are making e-commerce purchases or watching a movie on Facebook, they are not doing so on a website
13 from which Facebook cannot collect data.

14 410. The problem, however, was that Facebook faced stiff competition in many of the sub-
15 verticals it entered. For example, Facebook faced Foursquare and Yelp in the locations sub-vertical; eBay,
16 Craigslist, and Amazon in e-commerce and classifieds; and streaming giant Netflix in the longform video
17 space.

18 411. But Facebook knew this. And it also knew that its alternate path to DTBE maintenance—
19 cutting deals—could be achieved with significant leverage and the right C-suite connections. This was a
20 lesson the company no doubt learned from its 2011-2015 Platform scheme.

21 412. Accordingly, beginning in 2016, Facebook's strategy to obtain the signal needed to
22 maintain its DTBE and Social Advertising monopoly was not necessarily to defeat its competitors in the
23 sub-verticals it entered. Indeed, doing so would cost Facebook far more advertising revenue from these
24 companies—many of whom were major Facebook advertisers, including eBay and Netflix—than
25 Facebook would likely gain from ruinous competition with each company on its respective home turf.

FILED UNDER SEAL

1 413. Moreover, Facebook was (and remains) first and foremost an ad business, and it had no
2 interest in controlling adjacent markets other than for the purpose of obtaining actionable social data—
3 namely, intent data—or to obtain revenues for its social advertising business.

4 414. Instead, Facebook’s strategy was to enter key sub-verticals that it did not already control
5 or maintain a major presence in—*e.g.*, e-commerce, location services, longform video—and then threaten
6 chosen market leaders in each subvertical with either ruinous competition or, in the alternative, collusive
7 cooperation. The chosen parties were, generally speaking, both market-leading data sources and close
8 corporate (and personal) familiars of Facebook and its top executives—the perfect recipe for illegal
9 collusion.

10 415. Thus, between 2016 and 2018, Facebook entered into at least three anticompetitive
11 agreements with market leaders that leveraged Facebook’s entrance in respective sub-verticals to
12 guarantee that Facebook (a) received social data that it could mine from third parties, strengthening the
13 DTBE and Facebook’s social advertising stranglehold; (b) received substantial advertising revenue that
14 fortified its monopoly position in the social advertising market; or (c) both. In exchange, Facebook would
15 cooperate—and even assist—the third-party it supposedly competed with in the sub-vertical.

16 416. Based on the documents produced thus far in this action, Facebook entered into
17 anticompetitive agreements of the nature described above with at least Foursquare, eBay, and Netflix. In
18 the case of the latter two counterparties, Facebook leveraged its close personal and professional
19 connections—including the presence of Netflix’s founder and CEO on Facebook’s Board of Directors
20 throughout the entire relevant period—to broker a collusive deal.

21 417. Put simply, beginning in 2016 (and extending to the present), Facebook used the leverage
22 it obtained from entry into key sub-verticals—including, as presently known to Plaintiffs, e-commerce,
23 location services, and longform video—to extract anticompetitive agreements from third parties
24 (including, as presently known to Plaintiffs, Foursquare, eBay, and Netflix), with the intent and effect of
25 maintaining and fortifying Facebook’s DTBE and concomitant Social Advertising monopoly. For most
26 of the companies Facebook moved against, the alternative to helping Facebook secure its dominant
27 position in social advertising was ruinous competition from one of the world’s most powerful
28

FILED UNDER SEAL

corporations in their own markets. Plaintiffs and the putative classes paid inflated prices for Facebook advertisements as a result of this anticompetitive conduct.

B. Facebook Enters into an Anticompetitive Data Agreement with Foursquare

418. From 2015 to 2016, Facebook was in increasing competition with nascent social network Foursquare. Foursquare's competitive edge—which Facebook predicted would grow exponentially more valuable in the next few years, and potentially impact social advertising—was its laboriously created database and data stream of location data, including its users' real-time location social data.

419. Facebook moved directly into Foursquare's location-based corner of social networking beginning in earnest on January 29, 2015, when it announced its own "Place Tips" product, directly competing with Foursquare's location-based recommendation engine.

420. Facebook expanded further into Foursquare's territory in 2016 and 2017, putting further pressure on Foursquare—which was rapidly raising capital to compete with Facebook.

421. At the same time, Facebook began negotiations with Foursquare to acquire its crown jewel—its Places database and location-based data stream, which Foursquare made available through its API.

422. On September 27, 2017, Facebook and Foursquare entered into an "Inbound Data Evaluation License Agreement," which allowed Facebook to examine Foursquare's data in connection with a potential deal to acquire or license Foursquare's most valuable data. (PALM-004862134.) The agreement allowed Facebook to peer into the location database and data stream of its nascent social networking rival.

423. On or about July 3, 2018, Facebook entered into a final agreement to license Foursquare's valuable location data. (PALM-007391984.) A June 29, 2018 e-mail from John Delacruz summarized the reasons for the deal:

Why are we licensing this data?

Data licensing is a key part of our strategy for improving the data quality of our Business / Places graph and for improving Local Search. The data will also benefit all the products built on top of our graph across the Family.

FILED UNDER SEAL**What markets will we receive data for?**

Foursquare will provide us with global data. Their top 20 countries ordered by record count are US, Turkey, Brazil, Indonesia, Russia, Japan, Mexico, Thailand, Malaysia, Germany, Italy, United Kingdom, Spain, Belgium, South Korea, Canada, France, Netherlands, Philippines, and India.

What data are we licensing?

We will be licensing their global point-of-interest (POI) dataset. The dataset contains 100+ attributes, including business attributes, location attribute, rich attributes (e.g., accepts credit cards, has parking), tips, and tastes for 58M entities.

What impact do we expect to see?

We expect to see improvements to business/place data quality, PVD, and Local Search. Based on our data evaluations, in the best case scenario, we would see significant percentage point PQI improvements in coverage (+18%), best category (+17%), category relevance (+5%), hours (+5%), and price range (+10%). Note that these are best case estimates assuming we are able to choose the best attribute value for each record. Actual gains will be lower, but will improve over time as we improve our ML infra. In addition, we expect to see additional gains in Local Search metrics based on the improved category data we will receive, as well as rich attribute data and content such as tips and tastes. Note we don't expect significant against to PVD quality as the scope of this deal does not include Foursquare's Place Shapes or Pilgrim Technology.

(PALM-007391983, at 84.)

424. The same e-mail summarized the specific terms of the deal with Foursquare:

Deal Terms**Data and License**

- Data deliverable: global POI data for 58M entities,
- Data attributes: 100+ attributes, including business attributes, location attributes, rich attributes (e.g., accepts credit cards, has parking), tips, and tastes
- License: FB & Affiliates. Perpetual right granted upon completion of term or full payment.
- Rights: Restricted on Data as delivered. Broad rights of Conflated Data.

FILED UNDER SEAL

- Restrictions: No Resale, Distribution of Raw Data. Current FB API caching policy and rate limits remain in effect for initial term, material changes to API policy present termination option to Foursquare (FB retains existing data in perpetuity in this case)

- Delivery: Full refreshes of all datasets, monthly

Fees & Payments Terms

- Initial Term: 4 years
- Facebook License Fees: \$1.9M/year (total \$7.6M)
- Payment Terms: Invoiced quarterly (\$475k)

(PALM-007391985.)

425. The agreement was a capitulation by Foursquare, after Facebook's entry in the location-based services sub-vertical with the announcement and development of its own Places Graph API. Faced with potentially ruinous competition from Facebook's would-be replacement for the Foursquare location API, Facebook and Foursquare negotiated a deal by which Foursquare could live on as a location-based data company, but could no longer realistically serve as a potentially competitive social network—or use Foursquare's location data edge on Facebook to scale out a serious competitor with Facebook in the sale of Social Advertising. Instead, Facebook used its competitive leverage to extract an effective exit by Foursquare from social networking and coopted perhaps the single most dangerous source of unique targeting data that could have armed a potential new (or expanded) Social Advertising competitor—Foursquare's rich location data repository and real-time location social data stream.

426. The ultimate terms of the Foursquare agreement were truly a capitulation: even a termination of the agreement due to a material API change left Facebook with a perpetual right to access and use Foursquare's most valuable data. The data would be refreshed monthly, and the data itself would include vital tips and tastes data, as well as other “rich attributes” that could be used by Facebook to target advertising by identity.

427. Facebook's entry into the location-based services sub-vertical had allowed it to extract Foursquare's data, neutralizing the threat that a rival (or Foursquare itself) could leverage Foursquare's API to build or expand a serious Social Advertising competitor. Now that Facebook had Foursquare's

FILED UNDER SEAL

1 valuable location data in hand—on the most one-sided of terms—a new (or expanded) entrant in the
2 Social Advertising Market would at most have access to a subset of the data in Facebook’s possession,
3 and a subset Facebook perpetually received in updated form every month.

4 428. By obtaining Foursquare’s Places data in 2017-18, Facebook had not only eliminated one
5 of its social networking rivals, it had prevented that rival’s valuable store and stream of location data
6 from being used by Foursquare or another entity to build or scale a social advertising business with a
7 unique targeting edge against Facebook—the very type of competition that could erode the DTBE and
8 threaten Facebook’s Social Advertising dominance. To the contrary, through its deal with Foursquare,
9 Facebook had strengthened the DTBE protecting its business by augmenting its store of location data,
10 and further foreclosed meaningful Social Advertising competition for the near future.

11 **C. Facebook Enters into an Agreement with eBay to Preserve Its Social Advertising**
12 **Monopoly and to Strengthen the Data Targeting Barrier to Entry**

13 **1. Facebook’s Announcement of Marketplace Causes Concern for eBay, and**
14 **eBay Threatens to Pull Ad Revenue Unless Facebook Siloed Data from eBay**
Ads.

15 429. The launch of Facebook’s Marketplace in 2016 directly pitted Facebook against one of its
16 closest historical partners—and a major Facebook advertiser—eBay.

17 430. Founded in 1995 as one of the first successful dotcoms, eBay in 2002 acquired ascendant
18 payments startup PayPal—founded by Peter Thiel, Facebook’s first investor and longtime Facebook
19 board member. The combined eBay / PayPal would exist until July 2015, when PayPal was spun out into
20 its own company; during this period, no tech company had closer connections to Facebook than eBay.
21 Facebook integrated PayPal as its first major payment provider, and the two companies intertwined
22 themselves in each other’s products for many years, even as Facebook outgrew its older companion in
23 terms of active users.

24 431. Indeed, even as Facebook prepared to launch its new “eBay killer” in 2016, two members
25 of Facebook’s Board of Directors had deep connections to eBay: Peter Thiel, who founded PayPal and
26 ended up selling it to eBay, and Marc Andreessen, who served on eBay’s board from 2008 until 2014.

FILED UNDER SEAL

1 432. And nearly every senior member of the team tasked with launching Facebook Marketplace
2 came to Facebook directly from eBay / PayPal—including its head, Facebook Vice President, Platform
3 & Marketplace Deborah Liu, dubbed *The Woman Building Facebook's eBay Killer* by Forbes. Liu had
4 joined Facebook straight from nine years at eBay, where she was given product ownership over
5 “Marketplaces” and led a cross-functional team to complete post-acquisition backend integration of eBay
6 and PayPal.

7 433. Working under Liu on Facebook’s Marketplace team were (among others), Senior
8 Director of Product Management Mary Ku, another longtime eBay / PayPal alum who joined Facebook
9 straight from the former company, and Data Science Director Ashish Nayyar, who was hired by Facebook
10 in May 2015 after eight years at eBay / PayPal.

11 434. Built by eBay alumni as an “eBay killer,” Facebook’s Marketplace product launched in
12 October 2016 with great fanfare as a C2C e-commerce platform whose core features overlapped directly
13 with eBay’s principal line of business.

14 435. This did not escape eBay’s notice.

15 436. When Facebook announced Marketplace in 2016, it consulted David Doctorow, a senior
16 eBay executive and its Head of Global Growth, who expressed concern regarding Facebook’s newly-
17 competing product and flagged the companies’ ongoing negotiation of a “Data usage agreement”
18 concerning “Ads and Marketplace.” (PALM-002815413, at 415.)

19 437. At the time of the announcement, Facebook and eBay were in CEO-level negotiations
20 about Facebook’s access to and use of data from eBay’s advertising, including from the Facebook Pixel
21 and from eBay’s apps. As Facebook Monetization Product Marketing Director Emma Rodgers recounted
22 in a September 28, 2016 e-mail:

23 We are also having some sensitive conversations with eBay right now
24 around conversion pixel and app events data (Simon [Whitcombe] is
25 leading those discussions with David Doctorow) so we are treading
26 carefully here.

(PALM-002815413, at 415.)

27 438. That day, Whitcombe provided an update:
28

FILED UNDER SEAL

We've been working with eBay for a few weeks on an amendment to their pixel agreement that gives them assurances that their signals won't be used in Marketplace. This is something that [eBay President and CEO] Devin [Wenig] has requested and we've been working directly with David Doctorow, their Global Head of Growth. The goal is to have David share a draft of our amendment with Devin on Friday at which time he'll also update Devin on the Marketplace C2C launch.

(PALM-002815413, at 414.)

439. After Facebook announced Marketplace, its executives and other high-level employees internally lamented the press coverage, which had immediately recognized and homed in on the fact that the product competed directly with eBay. This was not a great look for Facebook's longtime business partner—and an important source of e-commerce signals data for Facebook's advertising business, which whom Facebook was presently negotiating a data agreement. Facebook's Emma Rodgers explained in an October 3, 2016 e-mail:

Yes, the press coverage is unfortunately heavily leaning on the competitive comparison. The competitive comparison definitely isn't an angle we proactively took with press but one they are making. While I tried to shift the press narrative to the organic activity happening on our platform, their interest in taking competitive spin isn't unexpected and was a key reason for the proactive outreach to our marketplace clients.

(PALM-002837128.)

440. On October 3, 2016, Facebook employees Aiden Roberts and Steven Bair drafted talking points for ads executive David Fischer's drafted talking points for an upcoming conversation with eBay President and CEO Devin Wenig. (PALM-010554150.) The talking points indicated that eBay had increased its advertising spend with Facebook consistently every year, and prepared Fischer for likely blowback from Wenig for Facebook's introduction of a directly competing C2C marketplace in eBay's bailiwick:

eBay Marketplaces Global Spend on FB

2014: \$38.6M

2015: \$57.8M (62% YoY growth; est. 4% of total budget)

2016 est. spend: ~ 80M+ (73% YoY growth; estl. 5% of total budget)

FILED UNDER SEAL

1 (Id.)

2 441. During negotiations, Facebook agreed to [REDACTED] to answer some of
3 eBay's questions about [REDACTED]. As the talking points noted:

4 As part of a long term pitch, [REDACTED]
5 [REDACTED] Their chief concern, directly from Devin, has
6 been around . . .

7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]

11 In order to be able to do so, [REDACTED]
12 [REDACTED] that helps assuage any fears Devin and
eBay have.

- 13 • Specifically, [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]

23 (Id. at 151.)

24 442. It was clear from CEO-level conversations that eBay feared that Facebook's Marketplace
25 would be a significant competitor—and one entering eBay's principal market at scale. The prospect of
26 ruinous competition was on the horizon, and eBay sought to leverage its data and advertising expenditures
27 to negotiate a competitive standstill.
28

FILED UNDER SEAL

1 443. Facebook Senior Director of Product Management (and eBay / PayPal alumna) Mary Ku
2 reported eBay's concerns to Facebook's Liu and other executives in an October 19, 2016, e-mail:

3 eBay is really freaked out about Marketplace. We knew this was a
4 possibility as we started building the product. Jon Eide had done an
5 estimate of potential revenue loss and presented to a subset of m-team. And
6 at a company level, we agreed that we were willing to take on the risk.
7 However, of course, we would like to mitigate that risk as much as possible.

8 eBay is most concerned about any of their data being used to help inform
9 what Marketplace does, and we are concerned that we will lose hundreds
10 of millions in current and potential revenue if we can't help them resolve
11 this. From a MP performance impact perspective, we are totally fine
12 excluding eBay data.

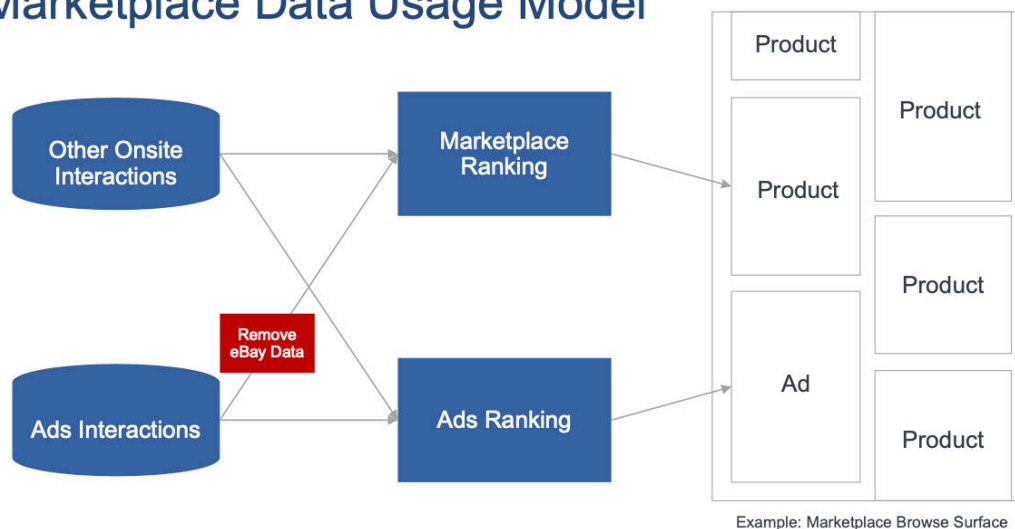
13 (PALM-005062864, at 867.)

14 444. Ku explained that although "the work to separate out their data into a different data source
15 is really costly," the task was "about preserving this revenue for the entire company. . . ." (*Id.*) Facebook
16 Director of Product Management Darshan Kantak, a computer engineer and data scientist, agreed with
17 Ku's assessment, noting that the "work to cleanse the data and retain the model is substantial." (*Id.* at
18 866.)

19 445. Although eBay's data was not a significant percentage of all data collected by Facebook,
20 siloing the data—particularly from trained AI and ML models—was a difficult engineering undertaking.

21 446. More problematic, Facebook's engineers were concerned with the precedent that would
22 be set if Facebook permitted eBay to opt out of Facebook's data pool.

23 447. An October 2016 internal Facebook presentation noted that although other advertisers
24 were concerned about the "competitive nature of Marketplace and data usage," eBay was the only
25 advertiser requiring Facebook "to take action at this point." (0076370576, at 578.)
26
27
28

FILED UNDER SEAL**Marketplace Data Usage Model**

448. The internal presentation (reproduced above) noted that Facebook would have to filter out eBay's data before it was fed to the Marketplace Ranking model. (*Id.* at 579.) The presentation recommended that such exceptions should only be made for large advertisers that make up a significant amount of a region's revenue. (*Id.* at 580.) According to the presentation, only three of Facebook's advertisers would potentially qualify for such treatment under such a standard: "eBay, Amazon, [and] Wish." (*Id.*)

449. By October 27, 2016, Facebook had prepared a draft term sheet for eBay's consideration. The background section of the term sheet set forth the problem:

eBay works with Facebook today to run advertising. In that partnership:

- eBay data is passed to Facebook via eBay's ad accounts and includes: product catalog content and event data from eBay's websites and apps
- Facebook additionally collects FB Ads Data on Facebook users' interactions (e.g., clicks) with eBay ads on Facebook.

Separately, Facebook builds Marketplace products:

- Marketplaces are Facebook surfaces primarily dedicated to enabling e-commerce transactions between buyers and sellers (exclusive of Facebook advertising)

FILED UNDER SEAL

- Facebook utilizes Marketplace Models to optimize the delivery of sales posts in Marketplace
- For the purposes of this discussion on Marketplace, [REDACTED]

(PALM-011266761.)

450. As the term sheet recognized, Facebook received data both from eBay itself and from users that interacted with eBay's ads. (See *id.*)

451. The term sheet proposed that Facebook would do the following "[i]n response to eBay's concerns:"

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

(*Id.*)

452. Internally, Facebook's marketing team balked at [REDACTED]. They regarded it as problematic for Facebook to [REDACTED]. More critically, the engineers tasked with [REDACTED] did not think it was technically possible to do so. The team discussed the matter in an internal chat:

Emma Rodgers (10/28/2016 14:15:53 PDT):

> Hi guys—check out my email coming out of Ads XFN. There's general discomfort in [REDACTED]. Simon, this has implications for your discussion with eBay.

FILED UNDER SEAL

Stephanie, I think you should circulate the proposed term sheet to Dan Rose, Fischer, Goldman to get alignment at that level on it.

Simon Whitcombe (10/28/2016 14:16:08 PDT):

> UGH

Emma Rodgers (10/28/2016 14:16:45 PDT):

> Yeah, Vlad raised a very important concern: [REDACTED]

Emma Rodgers (10/28/2016 14:17:08 PDT):

> Of that's the case, [REDACTED]

Simon Whitcombe (10/28/2016 14:17:13 PDT):

> I'm afraid we are likely done with eBay then. [REDACTED]

Simon Whitcombe (10/28/2016 14:17:29 PDT):

> which I need to tell him

Stephanie Wang (10/28/2016 14:17:34 PDT):

> Yep I'm writing an email to you guys saying as much re: [REDACTED]

Simon Whitcombe (10/28/2016 14:17:41 PDT):

> 100% certain of this

Simon Whitcombe (10/28/2016 14:18:07 PDT):

This is wrong

(PALM-009478444.)

453. Rodgers proposed escalating the team's concerns, particularly the concern that the task was impossible for the engineering team to accomplish:

Emma Rodgers (10/28/2016 14:19:21 PDT):

> K – we need to elevate the process on this one then. No one was comfortable committing to something that's not technically possible (of course). So, if this does mean we will lose eBay then we'll need 1).

FILED UNDER SEAL

1 Commitment from Ads product leadership to partner with Mary's team to
2 figure out if we can solve the technical limitation, 2) Commitment from
3 Fischer and [Facebook Vice President] Carolyn [Everson] that this is
4 important enough to do this.

(*Id.*)

5 454. One member of the team, Associate General Counsel Susan Sher, warned that even if
6 Facebook excluded eBay's product catalog information from the models running Marketplace, the
7 metadata would still be incorporated: "One thing to note is that even if we agree to not directly use product
8 catalog to inform marketplace, product catalog metadata goes into ads." (*Id.* at 446.)

9 455. The matter continued to escalate, and by November 8, 2016, eBay's board was threatening
10 to pull advertising spend from Facebook. Moreover, there were technical hurdles to removing eBay's
11 data from the AI / ML models used for Marketplace. As Stephanie Wang explained in a November 8,
12 2016, e-mail to Facebook Vice Presidents Dan Rose and John Lagerling:

13 As you may know, our recent launch of Marketplace featured strong
14 Facebook vs eBay headlines and exacerbated eBay's concerns around data
15 usage by Facebook. Their primary worry is that we will use the data they
16 send us for advertising purposes to bootstrap our competitive Marketplace
17 product.

18 We believe eBay's concerns are reasonable since our teams do apply ad
19 learnings to personalize Marketplace listings. The key challenge for us in
20 answering their concerns, however, is technical—we have no blocks
21 between Ads/Commerce data, and something like clicks (which we view
22 as Facebook data) is fundamentally embedded into Facebook models.

(PALM-003227822.)

23 456. Notably, Wang warned that eBay's concerns risked \$150 million in ad revenue to
24 Facebook:

25 eBay CEO Devin Wenig is now asking for concrete protections in writing
26 for Facebook and affiliates. eBay board concerns are strong enough such
27 that their teams have intimated they will pull Q4 ad spend if we do not get
28 to mutually agreeable terms. At stake: \$150M revenue forecasted for Q416
and FY2017.

(*Id.*)

FILED UNDER SEAL

1 457. On November 8, 2016, Dan Rose asked Stephanie Wang whether Mark Zuckerberg had
2 signed off on the company's proposals to eBay, and Wang committed to "get confirmation on where
3 things stand with Sheryl and Mark, and update this group." (*Id.*)

4 458. Negotiations continued into the next year, and by February 2017, eBay and Facebook were
5 considering specific language for a potential agreement. In a February 8, 2017, email, Wang recounted
6 eBay's latest proposal for contractual language:

7 As you may know we're in the middle of a negotiation with eBay on [REDACTED]
8 [REDACTED]. This was triggered by the public launch of
9 Marketplace—as you can imagine, [REDACTED]
10 [REDACTED].

11 One of eBay's asks is around [REDACTED]
12 [REDACTED].

13 (PALM-008351146, at 648.)

14 459. In that same email, Wang further queried whether eBay's custom audiences data was being
15 used by Facebook to assess a user's value. (*Id.*)

16 460. In response, Facebook Research Scientist Anand Bhalgat explained:

17 [W]e do use all bids to decide the user-value (userAvgMonthlyEcpm, as
18 well as some of the recent reserve price logic in feed ads) for various levers
19 in both feed and IG (Lei, David to Confirm).

20 (*Id.*)

21 461. In other words, eBay's proposal was problematic because Facebook's ad framework used
22 ad response data from its advertisers, including for eBay ads, to assess how much a user was likely to
23 spend on purchases—the user's value.

24 462. By March 3, 2017, eBay and Facebook appeared to have reached an agreement. (PALM-
25 011808391, at 392.)

FILED UNDER SEAL**2. The Facebook and eBay Agreement Not to Compete with Each Other**

463. In a March 3, 2017 e-mail, Stephanie Wang reported to Deborah Liu, Mary Ku, David Fischer, and Facebook Ads Vice President Rob Goldman (another eBay alumnus), with many others copied, that eBay and Facebook had “now gotten to what both sides believe is the final agreement.” (PALM-011808392.) Wang set forth a summary of the agreement, but first provided a “Context refresher” about the eBay and Facebook issues:

Context refresher: Facebook’s public launch of Marketplaces exacerbated eBay concerns around Facebook data. eBay’s worry is that we will use the data they send us for ads purposes to bootstrap competitive commerce experiences across Facebook. As a result, eBay’s CEO asked for concrete protections, in writing, to get to comfort with our ongoing advertising relationship while we simultaneously compete with their core business. At risk: \$150M+ in spend.

(*Id.* (italics in original).)

464. Wang continued by summarizing the terms of the deal by product area:

COMMERCE/MARKETPLACES

[Approved: Marketplaces, IX, IW]

These are obligations for any Facebook marketplace that involves aggregated sales listings between sellers/buyers. Not included: any affiliates, Ads, NF, Pages, Groups, Profile:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FILED UNDER SEAL

(PALM-011808392, 92-93 (bold, underlining, and ellipses in original).)

465. As Wang noted, the agreement prevented Facebook from

. In other words, Facebook impaired its position in Marketplace to strengthen its data targeting capabilities and models in its social ad business.

466. Wang continued, describing restrictions as to eBay's product catalog:

PRODUCT CATALOG

[Approved:]

The restrictions here are purely about

(*Id.* (bold, underlining, and ellipses in original))

467. Notably,

(*Id.*)

FILED UNDER SEAL**3. Facebook's Agreement with eBay Impaired Its Marketplace Product and Strengthened Its Core Ad Business**

468. Facebook's agreement was notable in what it exempted—

. As Wang explained:

Not in scope: While we pushed back on many eBay asks, these stood out...

(PALM-011808393 (underling in original).)

469. In June 2019, Facebook prepared an internal presentation that, among other things, attempted to quantify the effects of the eBay agreement. Facebook's internal data made clear that the agreement had resulted in a significant decline in the number of Pixel events and share of Pixel events data that eBay contributed to Facebook's data pool:



(PALM-008915674.)

FILED UNDER SEAL

1 470. It was clear that Facebook was allowing eBay to contribute comparatively less to the data
2 pool underlying Facebook's models, including by prohibiting the use of eBay's data in the Marketplace
3 targeting AI and ML models. (*See id.* at slide 4.) This meant that eBay would obtain the benefit of other
4 advertisers' data, but would have to contribute very little of its own to the pool, disadvantaging other
5 advertisers.

6 471. By entering into the agreement, however, Facebook ensured that its market power in the
7 Social Advertising Market was not just maintained, but strengthened. First, Facebook could use eBay's
8 valuable data, including purchasing signals, to optimize ads across its business, strengthening the DTBE
9 and helping forestall entry or expansion by any other Social Advertising source (especially one with a
10 trove of e-commerce signals). Second, eBay continued to pump hundreds of millions of dollars in ad
11 revenue into Facebook's core ad targeting business, directly backstopping demand and prices.

12 472. The net effect of the agreement was that Facebook and eBay agreed not to compete with
13 each other in their core businesses. Facebook would impair the data targeting for its Marketplace
14 product—the competitive lifeblood of that nascent business—and eBay would bolster Facebook's ads
15 product in exchange, contributing powerful signal data and hundreds of millions of dollars in ad
16 purchases. The agreement between Facebook and eBay increased the pool of social data powering
17 Facebook's ad business, strengthened the DTBE, and provided Facebook with increased revenue—all of
18 which helped Facebook maintain its monopoly position in the Social Advertising Market.

19 **D. Facebook Enters into an Anticompetitive Data Sharing Agreement with Netflix**

20 **1. Reed Hastings and the Facebook-Netflix Relationship**

21 473. eBay was not the only Silicon Valley giant with longstanding, board-level connections to
22 Facebook.

23 474. In 1997, Reed Hastings, a Stanford-trained computer scientist, left his job as CTO of a
24 large debugging company to found Netflix, a startup that combined two emerging technologies—DVDs,
25 which were just beginning to replace VHS cassettes, and a website to order them from. However, as
26
27
28

FILED UNDER SEAL

1 Netflix rapidly grew and began receiving large amounts of data from its subscribers' online choices and
2 actions, the company rapidly pivoted to a machine learning and AI juggernaut.

3 475. With the growth of streaming video as a preferred method of consuming premium
4 Hollywood-style content, Netflix rapidly scaled up both its content library and its backend ML / AI
5 systems to form an entirely new player straddling both the Silicon Valley tech industry and Hollywood-
6 style entertainment: a movie and television studio with a world-class ML / AI brain driving decisions
7 both online and off.

8 476. By 2016, Netflix had created a new type of tech juggernaut—the premium video
9 streamer—that was attracting increasing amounts of online revenue, attention, and valuable signals data.
10 Facebook, which was aggressively searching out signals for its ads business to maintain its DTBE after
11 the demise of the Platform, took notice.

12 477. However, there was a complication: Reed Hastings, Netflix's founder, Chairman, and co-
13 CEO, was a member of Facebook's Board of Director's, and had been since 2011.

14 478. Indeed, Hastings was more than just a long-term member of Facebook's Board; until 2019,
15 he was Chair of the company's special Compensation and Governance Committee.

16 479. Facebook's Compensation and Governance Committee was a closely-regulated
17 committee charged with monitoring and approving executive compensation, evaluating conflicts of
18 interests, and, as of July 2017, evaluating proposed changes in the Facebook's "Compliance with Laws
19 – Competition" update to the company's Code of Conduct. (*See* PALM-011953897, at 909-11.)

FILED UNDER SEAL**facebook****Proposed Update to Code of Conduct**
(see Appendix for redline)

Key Changes	Rationale/Notes
<u>Conflicts of Interest.</u> Removes travel and lodging from list of generally permissible items given to government officials. <u>Compliance with Laws.</u> <ul style="list-style-type: none"> - Lobbying & Campaign Finance: Adds political contributions to list of relevant Facebook activities. - Competition: Provides detail on the purpose of applicable laws and more direct guidance regarding price fixing, customer/territorial allocation, and group boycotts. 	The proposed update conforms to current approach of providing travel and lodging to government officials in exceptional cases only. <ul style="list-style-type: none"> - Making clear political contributions trigger campaign finance laws. - The proposed update provides additional information about competition and antitrust laws and clarifies certain conduct, both unilateral and joint, that can raise issues.

(Id. at 911.)

480. Besides Reed Hastings (who was the Committee's Chair), the other two members of the Facebook Compensation and Governance Committee between 2015 and early 2019 were Peter Thiel (the PayPal founder who sold his company to eBay) and Marc Andreessen (the former eBay board member). These three men had direct control over, among other things, corporate governance guidelines and policies, including those governing conflicts of interest and compliance with antitrust laws (*see id.*); the compensation of Mark Zuckerberg, Sheryl Sandberg, and Chris Cox (*see* PALM-011953897, at 931-49 (Hastings, Thiel, and Andreessen sole board members in compensation review for Zuckerberg, Sandberg, and others)), and a controversial 2016 plan to restructure Facebook company stock so that Mark Zuckerberg could liquidate his equity while still maintaining a controlling interest in the company (*see* PALM-01109282, at 282-93 (Apr. 22, 2016 Board of Directors Meeting re: Class C Reclassification Proposals) ("Pursuant to Delaware law, Mark Zuckerberg may have a material interest in the proposals related to the Class C reclassification . . . Neither Mark Zuckerberg nor the other employee directors will participate in the discussion and approvals of the Class C reclassification proposals.")).

FILED UNDER SEAL

481. Given the sensitivity of the issues overseen by the Compensation and Governance Committee, members of that Committee had to be expressly approved by the full board, with an eye toward federal legal requirements of independence for its members:

facebook

Compensation & Governance Committee Independence and Membership

- Proposal: recommend that the Board re-appoint Reed Hastings (Chair), Marc Andreessen and Peter Thiel as members of the Compensation & Governance Committee, effective immediately following 2017 Annual Meeting
- Proposal: recommend that the Board approve the above directors as (i) independent for purposes of rules governing compensation committees, (ii) “non-employee directors” pursuant to Rule 16b-3 of the Securities Exchange Act, and (iii) “outside directors” pursuant to Section 162(m) of the Internal Revenue Code

(PALM-011953897, at 908.)

482. Additionally, Facebook’s own corporate charter requires of its Compensation and Governance Committee:

The Committee will consist of two or more members of the Board, with the exact number determined from time to time by the Board. Each member of the Committee must:

- be an “independent director” as defined under the applicable rules, regulations and listing requirements of the stock exchange upon which the Company’s securities are listed for trading (the “Exchange Rules”) and must also satisfy the enhanced independence requirements for members of the compensation committee under the Exchange Rules;
- be free from any relationship that, in the opinion of the Board and the Committee, would interfere with the exercise of independent judgment as a Committee member;
- not be an executive officer or employee of the Company; and

FILED UNDER SEAL

- meet any other requirements imposed by applicable law, regulations or rules, including rules and regulations promulgated by the Securities and Exchange Commission (the “Commission Rules”), subject to any applicable exemptions and transition provisions.

483. The reason that members of Facebook’s Compensation and Governance Committee were required to meet strict independence requirements was that the issues that this Committee was charged with governing—the Company’s compliance with antitrust laws, the compensation of its top executives, and indeed the very ownership structure of the company—could not allow for even the hint of internal or external collusion or pressure. As Facebook explained in a February 2016 internal presentation:

facebook

Determination of Director Independence

- Pursuant to applicable rules and regulations and Facebook’s Corporate Governance Guidelines and other governing documents:
 - Majority of Board members must be independent
 - Each member of the Audit and Compensation and Governance Committees must be independent
 - Audit Committee members must meet special “super-independence” requirements under SEC rules
 - Compensation and Governance Committee members must meet special requirements

facebook

Determination of Director Independence (cont.)

- Broadly consider all relevant facts and circumstances
- Consider the issue not merely from the standpoint of the director, but also from that of persons or organizations with which the director has an affiliation
- Material relationships can include commercial, industrial, banking, consulting, legal, accounting, charitable and familial relationships, among others
- The concern is independence from management. Ownership of even a significant amount of stock, by itself, is not viewed as a bar to an independence finding

(PALM-011831146, at 182-83.)

FILED UNDER SEAL

484. In fact, Facebook listed as one bright-line “disqualifying circumstance” a situation in which a would-be independent director was a “partner, controlling stockholder, or executive officer of any organization . . . to which Facebook made, or from which Facebook received, payments for property or services this year or any of the past three years that exceed the greater of 5% of the recipient’s consolidated gross revenues for that year or \$200,000” (PALM-001831146, at 184.)

485. This raised internal red flags for Reed Hastings—who was the founder, Chair, and co-CEO of Netflix—as early as 2016, given Netflix’s then-\$73 million annual ad spend at Facebook:

Director Independence Matrix

Requirement	Marc Andreessen	Erskine Bowles	Susan Desmond- Hellmann	Reed Hastings	Peter Thiel
Director or family member cannot have a relationship that could interfere with the exercise of independent judgment	Board/ Committee decision	Board/ Committee decision	Board/ Committee decision	Board/ Committee decision	Board/ Committee decision
Director cannot be an executive officer or employee, and family member cannot be executive officer, now or within past 3 years	Ok	Ok	Ok	Ok	Ok
Director or family member cannot have received compensation over \$120,000 in any 12 month period within the past 3 years other than for board or committee service or service by a family member as a non-executive officer employee	Ok	Ok	Ok	Ok	Ok
Director or family member cannot be a partner, controlling stockholder or executive officer of any organization to which Facebook made, or from which Facebook received, payments for property or services this year or any of the past 3 years that exceed the greater of 5% of recipient’s consolidated gross revenues for that year or \$200,000	Ok	Ok	Ok	Netflix \$73M	Ok
Director or family member cannot be employed as an executive officer of another entity where, at any time during the past 3 years, any of the executive officers of Facebook serve on the Compensation Committee of the other entity	Ok	Ok	Ok	Ok	Ok
Director or family member cannot be a current partner of Ernst & Young and has not been a partner or employee of Ernst & Young who worked on Facebook’s audit at any time during past 3 years	Ok	Ok	Ok	Ok	Ok

(PALM-011831146, at 190.)

486. The situation only got worse over the next three years, as Facebook introduced a directly competitive premium video product, Watch, and Netflix increased its annual Facebook ad spend to over \$150 million. Nonetheless, Hastings remained on Facebook’s Board throughout this entire period—not merely as an “independent” board member, but as Chair of Facebook’s Compensation and Governance Committee, where he rewrote Facebook’s antitrust guidelines; set Mark Zuckerberg’s and Sheryl Sandberg’s compensation for 2016, 2017, 2018, and 2019; and approved a controversial (and widely

FILED UNDER SEAL

1 objected-to) reclassification and restructuring of Facebook’s Class C stock to give Zuckerberg majority
 2 control of the company even if he liquidated billions of dollars of equity.

3 487. Hastings’ position between 2016 and 2019 allowed him—and Facebook—to turn direct
 4 competition between Facebook Watch and Netflix into a collusive deal that divided markets between the
 5 companies, and bootstrapped Facebook’s DTBE and its Social Advertising monopoly at the expense of
 6 its Watch product, as described below.

7 **2. Facebook’s Entry at Scale Threatens Competition with Netflix**

8 488. When Facebook launched its Watch streaming video service in August 2017, it was
 9 immediately perceived as competitive with Netflix. Indeed, Watch’s offerings appeared to fit squarely
 10 within the scope of the premium, longform content primarily consumed on Netflix.

11 489. On September 8, 2017, the Wall Street Journal reported on Facebook’s entry into
 12 streaming video, noting that the new offering pitted Facebook directly against video services run by HBO,
 13 Amazon, and Netflix:

14 The social-media giant is willing to spend as much as \$1 billion to cultivate
 15 original shows for its platform, according to people familiar with matter.
 16 The figure, which could fluctuate based on the success of Facebook’s
 17 programming, covers potential spending through 2018, one of the people
 18 said.

18 The investment would far outpace Facebook’s previous outlays on video
 19 content, including its live-video deals last year. It also signals Facebook’s
 20 readiness to spend more than before to become what Chief Executive Mark
 21 Zuckerberg calls a “video-first” platform.

21 Facebook’s thirst for video content pits it against traditional broadcasters
 22 such as Time Warner Inc.’s HBO and deep-pocketed tech companies such
 23 as Amazon.com Inc. and Netflix Inc., which all are banking on video to
 24 capture the fleeting attention of users and seize billions of dollars in
 25 advertising that is expected to migrate from television to digital video.
 26 Apple Inc. is preparing its own billion-dollar war chest for content.

27 490. Facebook’s entry into the space meant that it would have to compete with Netflix for high
 28 quality content, particularly for full length dramas and TV shows. Publicly, the immediate question was
 whether Facebook could obtain enough original content to compete with Netflix.

FILED UNDER SEAL

491. Unlike Netflix, which was subscription supported, Facebook’s business model relied on ads, creating additional questions as to whether it could attract viewers away from other ad-based content providers, like cable companies. Moreover, Facebook would have to transition from short clips to full-length movies and TV shows.

492. Facebook sent its Vice President of Partnerships, Dan Rose, to interview with *Variety*. Rose told *Variety* that “hundreds of shows will be on Watch” within a week from launch and “then thousands will blossom really soon.” Rose explained that Facebook planned to fund original content until advertising revenues could support the new streaming video service:

Obviously, creating premium episodic content is expensive. Until we have a large enough audience—so the advertising revenue can cover the cost of creative—we helped fund some of them, so people see something when they go to Watch.

493. Internally, Facebook had determined that a significant expense of building a streaming video platform came from licensing content, such as popular TV shows. As an August 17, 2017, internal Facebook presentation explained:

Licensed content. Licensed content (e.g., *Friends*, *Seinfeld*) draws more eyeballs than original content. For example, on Netflix, at any given time, more than 75% of streams are of licenses content. This is a meaningful revenue source for content owners and a meaningful cash outlay for platforms.

(PALM-006842466, at 78.)

494. Netflix was rapidly weaning itself from licensed content by investing heavily in original content. Facebook internally did a competitive analysis of Netflix and noted that the company was “burning through its cash” but was developing original content that was better than other platforms’:

Advantages [Netflix]:

- **Netflix is the leading SVOD**, with more subscribers and daily WT than other subscription based competitors (including TV networks).
- **Netflix’s original content performs better** than the original content of other platforms.

FILED UNDER SEAL

- Netflix is growing its backlog of original content, **reducing its long-term dependency on licensing content** (which is expensive). Data helps inform what original content to create and what licensed content to buy / renew.

(PALM-006842466, at 524 (bold text in original.))

495. As Facebook’s competitive analysis noted, one of Netflix’s major advantages stemmed from the data it collected from its users. That data informed Netflix’s content acquisition and creation strategy. User behavior would directly indicate whether licensed content was worth acquiring. Likewise, user watch time and behavior informed what sort of original content Netflix created. This was data that Facebook did not yet have as part of its nascent streaming video system.

496. Nonetheless, Jon Eide, who authored the internal August 2017 Netflix competitive analysis, recommended that Facebook invest in original content to avoid dependency on licensing content at high prices—and to better develop unique data signals around its original content that would not be shared by video competitors. (*See* PALM-006842466, at 524.)

497. Facebook noted that its new service had an additional problem—the behavior of Facebook users. Those users were accustomed to shorter clips on their news feeds, not full-length videos. Facebook, however, needed to maximize watch time in order to extract valuable user behavioral / social data for its advertising ML and AI systems. As Eide explained, Facebook user behavior would have to change for Facebook’s Watch to be successful: “While almost a billion users watch video on Facebook daily, watch times and average session times are low as compared to key competitors.” (PALM-006842466, at 517.)

498. Facebook’s task was clear: if it was truly to compete with Netflix, it would have to move heavily into longer, feature-length films, as well as original content.

3. Facebook and Netflix Enter into Amended Agreements

499. There were numerous internal problems with Facebook’s new Netflix-killer.

500. First, Netflix had long been a partner with Facebook. After the April 2015 public deprecation of the Friends and Newsfeed APIs, Netflix was given an exemption. Netflix also provided Facebook with sensitive customer relationship management (“CRM”) data when it ran ads and Facebook needed to track ad conversions. (PALM-007621101, at 10.)

FILED UNDER SEAL

501. Netflix also partnered with Facebook to create content promoting its shows on Facebook. For example, Netflix and Facebook collaborated to promote Netflix shows, like Narcos, an original TV show produced by Netflix about Pablo Escobar. Facebook internally described the collaboration to Sheryl Sandberg in a January 2018 brief:

Collections + Canvas: Netflix approached our team with a challenge for Narcos S3: find innovative ways to get Pablo fans excited about the power of the new drug kings, the Cali Cartel. Leveraging our Collection + Canvas format, we pitched an interactive “trivia style” feed unit which revealed the answer (and trailer) in a single-screen canvas. Netflix produced regional versions and promoted over global launch weekend in 14 countries.

(PALM-008530032.)

502. And, when Facebook rolled out new APIs, it hand-selected Netflix to help test them. For example, on October 15, 2017, Facebook’s Konstantinos Papamiltiadis invited Netflix to integrate with Facebook using the new “Mentions” API:

Hello team Netflix,

As we look to add more capabilities to the Instagram Graph API (currently we provide comments moderation and insights), we would like to invite you to integrate future API features and provide early feedback.

Starting in Q4 2017 we are building a “Mentions” API that will allow you to pull organic posts which mention your company in the caption or comments and respond to them.

We’re only opening it up to a handful of partners to start, and wanted to see if you’d be interested in getting early access?

Let me know if you would like to set up a call to discuss this opportunity in detail.

(PALM-004821849.)

503. Second, Netflix was a major advertiser on Facebook. In a January 16, 2018, brief to Sheryl Sandberg, Facebook reported that Netflix had “invested” hundreds of millions of dollars in Facebook through advertising spend, which was expected to increase in 2018:

FB Investment

FILED UNDER SEAL

- 2016: \$149M, 113% YOY, ~23% of overall mktg budget
- 2017: \$169M, 13% YOY, 27% of overall mktg budget
- 2018: \$200M Global JBP, 19.5% YOY, ~28-30% of overall mktg budget

(PALM-008530031.)

504. Finally, as noted above, Netflix’s founder, Chairman, and co-CEO, Reed Hastings, sat on Facebook’s board. Facebook’s incursion into Netflix’s core business was not lost on Hastings—or his company.

505. Facebook took pains to assure Netflix that it was not directly competing with it. At prior earnings calls, Sheryl Sandberg had gone so far as to state that Facebook was not taking on Netflix because “we are a platform, not a video service” and that Facebook was “funding [content on Watch] to kickstart the ecosystem.” (PALM-006172689.)

506. But internally, Facebook knew better—and so did Hastings. The situation deteriorated to the point where, in January 2018, Sheryl Sandberg had to have a “Fireside Q&A” at Netflix in which she and Hastings were to “teas[e]”, in front of “500 senior [Netflix] people” (with “Strict no recording”) about how Sandberg had “driven [Facebook] into more direct video competition with us, was it something I said?” (PALM-003207836 (questions/script provided by Hastings to Sandberg in advance).)

Netflix Fireside Q&A

Overall style in moving back and forth between personal get-to-know Sheryl questions and intellectual/political questions. 500 senior people. Strict no recording.

Intro: Disney board, Facebook board/exec, (teasing) you’ve driven both companies into more direct video competition with us, was it something I said?

Let’s start early. Can you tell me about middle school and high school? What were you like?

(Id.)

507. The January 2018 “Fireside Q&A” at Netflix joked that the “[o]nly topic [Hastings] wo[uldn’t] ask [Sandberg] about” in front of Netflix’s upper management was “FB professional video strategy”

FILED UNDER SEAL

Additional questions

- What is your earliest memory of being called Bossy?
- Only topic I won't ask you about is FB professional video strategy, OK?
- How did Lean In change your life (Ted talk and book)
- For women graduating college today how will things be different than when you graduated?

(*Id.* at 837.)

508. But behind the scenes, the two companies were doing quite a bit of talking about just that.

509. By the third and fourth quarters of 2017, Facebook and Netflix appeared to have reached a détente. The companies entered into several agreements, sometimes styled as addendums to existing agreements, that purported to limit Facebook's ability to train its AI and ML based on the information Netflix's ad campaigns generated and information Netflix provided to Facebook.

510. For example, on August 15, 2017, the companies executed an Addendum to their Advanced Measurement Beta agreement that [REDACTED]

[REDACTED]:

[REDACTED]

(PALM-008914377.)

511. Days later, on August 21, 2017, Facebook and Netflix entered into an addendum to the Offline Conversions Agreement. On November 1, 2017, Facebook and Netflix again amended their Advanced Measurement Agreement. On April 1, 2018, Facebook and Netflix amended their Terms for

FILED UNDER SEAL

1 Conversion Tracking, Custom Audiences from Your Website, and Custom Audiences from Your Mobile
2 App” agreement.

3 512. The upshot of the above agreements was that Facebook agreed to segregate its Watch
4 product from its most powerful AI and ML systems, in order to assure Netflix that Netflix’s own video
5 data would not be used to fine-tune Facebook’s new premium video product.

6 513. In return, Netflix would permit Facebook to use some of its most powerful data signals in
7 Facebook’s ad-targeting systems and models, and it would continue to spend hundreds of millions of
8 dollars on Facebook advertisements.

9 514. After the execution of these agreements, Facebook flipped from potentially ruinous
10 competition with Netflix on Netflix’s home turf to overt cooperation. More conspicuously, Facebook
11 gerrymandered its own Watch product around Netflix’s core business, abandoning much of its original
12 and feature-length content. The companies’ less-than-arms-length relationship had paid off: Facebook
13 gotten what it wanted (Netflix signals for its ad targeting systems, and continued Netflix ad spend), and
14 Netflix had gotten what it wanted (Facebook’s near-term exit from premium, longform video content).
15 However, those paying supracompetitive prices for Facebook ads because of the DTBE were not
16 benefitted, and indeed were harmed, by the Facebook-Netflix agreement.

17 **4. Facebook and Netflix Agree Not to Compete in Each Other’s Market.**

18 515. What followed the series of agreements and addenda between Facebook and Netflix in
19 2017 and 2018 made clear the scope of the companies’ agreement. Facebook cut out portions of its Watch
20 product that competed with Netflix; Facebook agreed not to use Netflix’s social data to power its
21 streaming video business; and Facebook developed a custom advertising AI / ML system for Netflix. In
22 exchange, Netflix pumped hundreds of millions of dollars of advertising into Facebook’s Social
23 Advertising monopoly and, with certain narrow exceptions, allowed Facebook to use its social data to
24 power the AI and ML systems that allowed Facebook to target advertising.

FILED UNDER SEAL

516. As explained below, the net effect of this agreement was Facebook's withdrawal from Netflix's core streaming video territory, and in exchange, Netflix helped Facebook strengthen its Social Advertising Market monopoly, including by enhancing Facebook's revenue and AI / ML technology.

517. To begin with, Facebook entered into an agreement with Netflix to build Netflix a dynamic advertising model. (PALM-008730853.) Facebook described the model in a July 31, 2018, document entitled, Dynamic Ads (Subscriptions)—Detailed Alpha Brief for Netflix:

Context

Dynamic Ads for Entertainment and Media (DAEM) is building a product that selects which set of titles from a client's media catalog will best drive conversion events for individual users, i.e., matching the right content title for each of the right users. Our goal is to test whether our new ranking models are able to move advertiser metrics and/or streamline the existing campaign creation/management process.

(PALM-008730853.)

518. Facebook was designing a bespoke system that targeted users with *Netflix* content such that a conversion event was likely to occur. This was precisely the sort of targeting Facebook would have needed to do to promote its supposedly competing Watch product. Instead of doing so for itself, Facebook was doing it for Netflix.

519. Facebook, however, received something in exchange that was more valuable to its Social Advertising monopoly—user intent data (and the underlying data to make predictions)—from Netflix. As the same document explained:

DYNAMIC Ads product value

Dynamic ads leverage cross-device intent signals to automatically promote relevant products from your entire catalog with unique creative, showcasing one or more products, across Facebook. Key benefits include:

- **Scale:** Generate a unique ad for each and every product automatically without having to configure each one individually
- **Personalization:** Show relevant products to users, based on interests they have shown on your site or interests they've shown on Facebook.

FILED UNDER SEAL

- **Always-on:** Set up your campaigns once, and continually attract shoppers more likely to convert.
- **Cross-device:** Serve the right product to the right user across devices (mobile, desktop or tablet), based on login, not cookies.

(PALM-008730853.)

520. The document further described how the product worked:

DAEM tries to select the best movie/tv show title from the catalog to show to the user in the ad creative. As of now, this personalization is completely power by various ways users engage with data and entities (media and non media) on Facebook. We also learn real-time from the performance of individual titles from your catalog as your campaign delivers.

(PALM-008730853, at 56.)

521. In short, Facebook's ad systems would target video content to users on Netflix's behalf, and in the process, Facebook's AI and ML would receive valuable social data to train on.

522. After initial testing of its new system designed for Netflix, Facebook prepared a postmortem report on December 19, 2018. The report concluded the following about Netflix's customer intent data:

User selection

Difference between CBO and DAEM where CBO implicitly bakes in title selection during user selection powered by strong exploration

Focus on identifying user's intent to subscribe to media content and use that as a signal to influence user selection

Focus on closing some systematic ranking gaps between the new DAEM product and CBO/standard FB delivery.

(PALM-008731246, at 48.)

523. Netflix continued to advertise through Facebook, and Facebook's AI and ML trained on the data obtained through the Netflix campaign. The only exception was Netflix's "title weight data," as the companies agreed that Facebook could not target advertising *solely* based on such data, but could otherwise use Netflix data to train its ML and AI:

Current custom partnerships that need to be upheld, contractually . . .

FILED UNDER SEAL

1 Netflix: No use of title weight data to (1) develop FB's own video-
 2 streaming product and (2) target ads SOLELY based on that title weight
 data.

3 (PALM-11129211, at 12.)

4 524. Facebook in essence agreed to impair its Watch and other streaming video products by
 5 agreeing with Netflix not to use certain data obtained in its advertising to develop those products. (*Id.*)
 6 In exchange, Facebook was allowed to incorporate data from Netflix's ads into its ad targeting ML and
 7 AI systems.

8 525. Facebook also gerrymandered its Watch product around Netflix's business. Although
 9 Facebook initially announced original content, feature length movies, and TV series, Facebook began
 10 canceling its content projects and reverted to publishing shorter clips on its platform. Facebook also
 11 scaled back on other long form content, such as news programming.

12 526. In December 2018, Facebook cut the funding for its news shows on watch. In February
 13 2019, Facebook announced that it would not be renewing most of its news programs. As *Digiday* reported
 14 on February 26, 2019:

15 Last June, Facebook rolled out its first set of daily and weekly news shows
 16 from publishers such as ABC News, CNN, Business Insider and NowThis.
 17 Overall, Facebook has launched 21 news shows on Watch including
 CNN's "Anderson Cooper Full Circle," BuzzFeed's "Profile" and
 Univision's "real America with Jorge Ramos."

18 In recent months, Facebook has been telling news publishers that it will
 19 only renew about a third of the existing news shows that it has funded for
 20 Facebook Watch, according to publishing sources that have met with
 Facebook.

21 527. Facebook also began cutting its original content, particularly its scripted series. In January
 22 16, 2020, Facebook cut popular shows *Sorry for Your Loss* which starred Elizabeth Olsen, and *Limetown*
 23 which was headlined by Jessica Biel.

24 528. By early 2020, Facebook had publicly canceled virtually every drama on its platform,
 25 including *SKAM Austin*, *Five Points*, *Sacred Lies*, *Turnt*, *The Birch*, and *Steroscope*. Facebook also cut
 26 its comedies, *Strangers* and *Queen America*. Facebook cut its docuseries, including *Humans of New York*:
 27
 28

FILED UNDER SEAL

1 *The Series, Bill Murray & Brian Doyle-Murray's Extra Innings, Tom vs. Time, Fly Guys, Behind the*
2 *Wall: Bubba Wallace, and Inside the Madness: Kentucky Basketball.*

3 529. Facebook cut its game shows, *Confetti* and *Outside Your Bubble*. Facebook also cut its
4 animation series, *Human Kind of*, *Liverspots and Astronots*, and *Human Discoveries*. Facebook cut
5 almost ever reality show, including *No Script with Marshawn Lynch*, *Relationshipped*, *Backcourt: Wade*,
6 *The Tattoo Shop*, *Bear Grylls: Face of the Wild*, *Help Us Get Married*, *Huda Boss*, *Sneaker Hustle*, *Troy*
7 *the Magician*, *You Kiddin' Me*, *Big Chicken Shaq*, *Double Take*, and *Will Smith's Bucket List*.

8 530. Although Facebook's chief monetization strategist Jon Eide had expressly recommended
9 in 2017 that Facebook acquire original content, and despite internal presentations that made clear that
10 Netflix's programming succeeded because its AI and ML systems allowed it to determine what viewers
11 wanted, as soon as Facebook and Netflix concluded their negotiations over data in early 2018, Facebook
12 promptly and consistently did the opposite.

13 531. That is, Facebook abandoned the use of data derived from Netflix's ads for its video
14 streaming service, which immediately handicapped Facebook's Watch targeting. This was because it was
15 difficult—and perhaps impossible—to segregate that data from the rest of the data pool from which
16 Facebook drew on to train its ad targeting models, leaving Watch with either an incomplete data set to
17 train its targeting system on or an inferior model to do the targeting.

18 532. Facebook also abandoned all of the original content it had paid for just a year prior. In
19 fact, Facebook near-immediately canceled all Watch programming that significantly overlapped with
20 Netflix's offerings.

21 533. Moreover, although Facebook internally determined that it needed to increase watch time
22 on Facebook for Watch to be successful, which required Facebook to add longer-form programming to
23 its service, Facebook did the opposite, focusing instead on shorter clips. These shorter clips were outside
24 of the scope of Netflix's programming.

25 534. Facebook had fully retreated from Facebook's territory and crippled its own Watch
26 product to do so. In exchange, Netflix allowed Facebook to train its models on its data and pumped large
27 amounts of advertising into Facebook's coffers.

FILED UNDER SEAL

535. Facebook had used the threat of ruinous competition from one of the world's most powerful companies to gain by agreement what Facebook would otherwise have had to compete viciously for on Netflix's home turf—an incredibly valuable trove of signals data for Facebook's ad business. In exchange, Netflix prevented another tech giant from entering its market in earnest. This helped to maintain and fortify the DTBE, secured Facebook's Social Advertising dominance, and in doing so harmed the Plaintiffs and the putative classes.

536. On April 12, 2019—a few months after the last aspect of the Facebook-Netflix agreement not to compete was memorialized, and as Facebook had begun in earnest to pull back from its investments in Watch—Facebook announced that Reed Hastings would be leaving Facebook's Board of Directors.

VIII. FACEBOOK ANTICOMPETITIVELY USED ONAVO DATA TO BUILD A MASSIVE, MACHINE LEARNING-DRIVEN SURVEILLANCE SYSTEM AND TO SPY ON FACEBOOK USERS EVEN WHEN USING NON-FACEBOOK APPS.

537. From 2016 through 2019, Facebook escalated its use of Onavo spyware to create the largest electronic surveillance system ever deployed by a private entity—and perhaps the largest surveillance apparatus ever deployed anywhere, by anyone. Facebook did so, in part, by deploying Onavo at scale against the user base Facebook had acquired through its Instagram and WhatsApp acquisitions—using data from Onavo spyware to validate machine-learning models designed to surveil user interactions with competitive apps.

538. During this period, Facebook used deceptive applications, such as a Virtual Private Network (VPN) app, to obtain privileged access to users' smartphones. With that access, Facebook surreptitiously took voluminous, hardware-level data from user cell phones, including call and video call logs, message logs, battery logs, and sometimes even more sensitive user information. Facebook, through Onavo, used that data to determine precisely which apps users were engaging with, and for how long.

539. In addition, Facebook used that same stream of data to match users it surveilled through Onavo with internal Facebook IDs. This matching process meant Facebook could spy on its own users as they used competitive apps.

540. The upshot of the above—including Facebook's use of deceptively obtained Onavo information to provide a “ground truth” baseline for the training of Facebook's probabilistic identity

FILED UNDER SEAL

1 matching models—was that Facebook used deception to obtain a competitive edge in ad targeting
2 between 2016 and 2019.

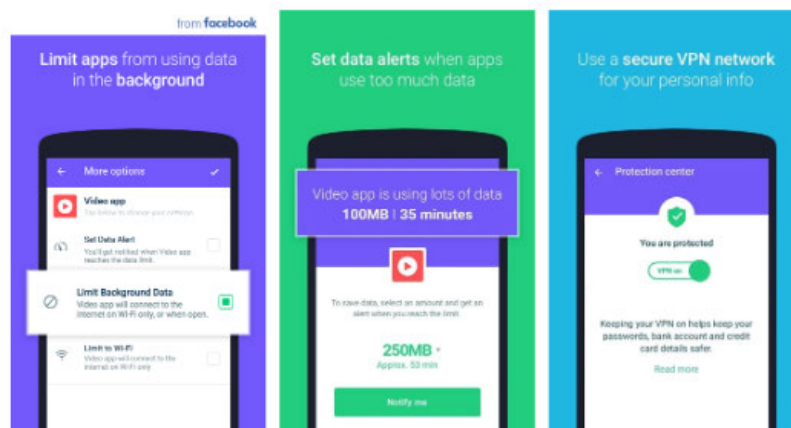
3 541. Facebook’s surveillance and matching system was derived from data secretly stolen from
4 tens of millions of iPhone and Android devices throughout the world. By doing so, Facebook strengthened
5 the DTBE protecting its business, not only by spying on Facebook’s own users, but by surveilling outside
6 threats to Facebook’s business.

7 542. This deceptive conduct, tied to a professional spyware apparatus of a scope and scale the
8 world had never before seen, provided Facebook with a further competitive advantage against would-be
9 entrants to the Social Advertising Market, helping to maintain the DTBE and to seal off any erosion of
10 Facebook’s Social Advertising market power—and concomitant supracompetitive ad prices—between
11 2016 and 2019. Plaintiffs and members of the putative classes were injured by this conduct.

12 **A. Onavo’s Spyware Secretly Shuttles Sensitive User Data to Facebook for Its Internal**
13 **Machine Learning Models.**

14 543. Onavo initially provided Facebook with analytics about competing apps. By 2016, Onavo
15 became something far greater—a real-time surveillance system. Onavo accomplished this by designing
16 software that appeared to provide a particular utility function, while at the same time transferring users’
17 data from their phones to Facebook for analysis.

18 544. One app Onavo leveraged was called Onavo Protect (internally referred to as iProtect for
19 iOS and aProtect for Android). The software was billed as a means of limiting apps from using data in



FILED UNDER SEAL

the background of a smartphone and as a provider of virtual private network (VPN) services, supposedly providing users with additional privacy as they traversed the Internet.

545. However, Onavo Protect did the opposite. It was, among other things, monitoring the data packets coming in and out of the user's device, transferring device logs, and monitoring app usage. The software was available on Apple's App Store and the Google Play Store, and was designed to spy on users on either iOS or Android devices. Facebook's Onavo also put out other apps designed to allow Facebook to monitor internet traffic and device usage, including the Onavo Bolt App Lock—an app that purported to lock other apps, yet in reality secretly stole away user and device data for Facebook's models.

546. By monitoring the data traffic in and out of the device, including through HTTP, SIP and DNS traffic, Onavo's apps allowed sensitive user data to be sent off to Facebook, where Facebook's data scientists devised machine learning models that made inferences about users and how much time they spent on various apps.

547. By April 2017, Onavo's packet tracking had become sophisticated, allowing Facebook to determine whether a user was sending iMessages with media included, as well as whether the user was using the Apple FaceTime system to make calls. As Facebook's Kieval Patel explained in an April 26, 2017, e-mail:

What we can detect are the media transfers since those use a unique user-agent over HTTP (samples of these can be viewed here: <https://fburl.com/b3pmi7xm>). . . .

I didn't mention it in my talk, but for Facetime app we also have a unique detection method. We track SIP protocol packets (sadly we can't capture all of them). With that we can report usage of video/audio calls including durations. Long ago, I presented that work – slides here (https://www.dropbox.com/s/ex0ypompog5oecs/facetime_sip_detection_v3.pptx?dl=0).

(PALM-005019528.)

FILED UNDER SEAL

1 548. By August 2017, Facebook’s Onavo team was enhancing its surveillance of iMessage
2 conversations by incorporating iOS power consumption logs with the iMessage data it was extracting.
3 (PALM-01130706, at 714.)

4 549. In January 2018, Onavo cracked the problem (*i.e.*, “sadly we can’t capture all of them”)
5 completely, and was working on obtaining ***actual user messages*** from iMessage. Facebook Product
6 Manager Erez Naveh reported on the breakthrough in a January 4, 2018 status e-mail:

7 1. iMessage – found a new way to track conversations on iMessage for iOS
8 < 11. For these devices, we think we’ll be able to see the actual messages
9 including what type of media is shared in iMessage conversations. This
10 will also include historical data (up to a few months) for each user we track.
11 We are now working on collecting this data from the devices. . . .

(PALM-004988332.)

12 550. Onavo had also found internal tables built into Apple’s iOS that provided information
13 about which apps were in the foreground of the device. As Naveh explained in the same e-mail:

14 2. Time spent measurement in iOS – found a new table in iOS that holds
15 events related to apps moving to foreground – we think this will help us
16 improve our time spent measurement. This table has some random time
17 shift in different devices. We are working on a way to compensate this time
18 shift to make this data usable.

19
20
21
22
23
24
25
26
27
28
(*Id.*)

FILED UNDER SEAL

551. Onavo was also spying on other commonly used apps, including the YouTube app, Snapchat, Android Messages, and Twitter. A January 29, 2018 e-mail from Facebook Director of Product Management – Artificial Intelligence Larry Weyer summarized the data obtained from various apps and the methodology used to do so:

	Confidence		Categories covered		Business Questions	Methodology
	Reach	Timespent	Actions			
YouTube	High	Medium	High	Video duration, time watched, video category	<u>YouTube: Key Competitor Tracking - Questions</u>	SSL bump (risk: works for iOS & Android M and below)
Snapchat	High	Medium	High	Discover, Maps, Snap, Stories, Chat	<u>Snapchat: Key Competitor Tracking - Questions</u>	SSL bump (risk: Snapchat are moving to SSL pinning in iOS)
Google Photos	High	Medium	High		<u>Google Photos: Key Competitor Tracking - Questions</u>	Usage stats, accessibility
iMessage	Low	Low	Low	Messages, message types	<u>iMessage: Key Competitor Tracking - Questions</u>	power logs"
Android Messages	High	Medium	High	TBD	<u>Android Messages: Key Competitor Tracking - Questions</u>	Usage stats, accessibility
Twitter	High	Medium	High	TBD	TBD	SSL bump, Usage stats

(PALM-004982075.)

552. Onavo also derived data from third-party apps that used a Facebook software developer kit ("SDK"). By using Facebook code, the underlying app would automatically import the Onavo's tracking mechanisms.

553. Onavo's apps, as well the Facebook SDK, were in fact Trojan Horses, designed to spy on user Internet traffic to determine how and how long users were using various apps on their devices. Facebook stored that data in an internal database system called, the "Hive," where the data could be queried across Facebook's organization.

554. Onavo continued secretly hoovering user data until Apple and Google removed Onavo's primary apps from their app stores in August 2018 and February 2019, respectively. Both Apple and Google determined that Facebook's Onavo apps failed to properly inform users that their data was being transferred to Facebook and used for machine learning and other models. Even with disclosure to users,

FILED UNDER SEAL

Facebook's practice of spying on user smartphones and devices through Onavo apps violated both Apple and Google's terms and/or policies.

B. Facebook Used Stolen Onavo Data Together with User Data from Its Own Apps to Build a Granular and Real-time Competitive Surveillance System.

555. By the end of 2016, Facebook had acquired both Instagram and WhatsApp. WhatsApp, in particular, provided Facebook a massive and global user base. Both apps provided Facebook with entry into tens of millions of smartphones and other mobile devices.

556. At the same time, Onavo struggled to obtain validation information about the data it collected on third-party apps, such as Snapchat or YouTube. Although Onavo was able to exfiltrate highly sensitive information from the users that had installed one of Onavo's spyware apps, the data Facebook obtained was only from a subset of users of major third-party apps that Facebook sought to surveil.

557. Onavo-collected user data, augmented by data collected through Facebook's own apps, allowed Onavo to make highly accurate inferences about the entire set of third-party app users. That is, Facebook's WhatsApp and Instagram apps not only provided Facebook with the ability to validate Onavo's data, but to build powerful machine-learning models that Facebook's data scientists could use to measure time spent on various third-party apps with unprecedented precision.

558. Facebook accomplished this by deriving what it called the "ground truth" from its own apps, including Instagram, WhatsApp, and the Facebook Blue App, then using that data to validate models built on Onavo data stolen from cell phones through Facebook's spyware.

559. When combined, these streams of data allowed Facebook to obtain a granular, real-time picture of precisely what apps users were spending time on and engaging with. By combining Onavo's spyware data with user data collected on Facebook's own apps, Facebook had built the largest real-time surveillance system in existence.

560. Not only could Facebook determine how much time users spent on their own apps, but it could determine what users were doing on other apps, including as to the media sent through other apps. In some cases, Facebook could spy on the content of messages sent or media sent or received on a user's device.

FILED UNDER SEAL

561. Facebook used this data to build machine-learning models that allowed it to make inferences about demographics. Specifically, Facebook could train machine learning and statistical models with high levels of precision that allowed Facebook to target users by age (which Facebook referred to as “life stage”), location, education, and other attributes. Facebook used these models to make inferences about users based on the data it collected.

562. For example, in a March 24, 2017 presentation, Facebook described building a model that better identified younger users, including minors, ages 13-18. Facebook was using Onavo to granularly model young users and to correct any biases in its data before it was used to train machine-learning models.

Project overview

- What we are trying to accomplish (high level):
 - Improve accuracy of estimates broken down by age and gender (user level accuracy is not a goal)
 - Align the data with the FB age affinity project
 - Provide more granularity (13-18, 19-22, 23+)
- If successful, the impact will be:
 - Better visibility into app usage behaviors of high school and college age users

(PALM-008796707, at slide 2.)

563. Those inferences and demographic information were then stored in Facebook’s Hive database, where the information could be readily queried or viewed through a portal system within Facebook.

C. Facebook Matched the Onavo Data It Collected from Users on Other Apps with their Facebook IDs and Stored User Data in Its “Hive” Database.

564. Facebook also used Onavo data to determine the precise identity of the users it was surveilling, if those users also had a Facebook account. Thus, a Snapchat user could be identified using

FILED UNDER SEAL

1 Onavo's spyware, and then Facebook would match that user's Onavo ID to their internal Facebook ID
2 ("FBID").

3 565. Facebook's internal documentation indicated that matching data was available by
4 querying fields on Facebook's Hive database, explaining that "Onavo users can be matched to their fbid
5 using the table dim_onv_fb_user_matchin." (PALM-009223604.)

6 566. Not only was personally identifying information about these users stored in the Hive, a
7 user's "clickstream" or sequence of actions on their device was also exfiltrated and stored, then associated
8 with their Facebook ID. As Onavo's Guy Rosen explained in a November 2016 post about extracting
9 information about what users were watching on YouTube: "On iOS we log full clickstreams so the request
10 should be there in the Hive table and querytable if we can decompose the video URLs." (PALM-
11 005101103.) Onavo continued to extract clickstream information from users' devices in 2017, 2018, and
12 most of 2019.

13 567. Onavo therefore provided Facebook another means to extract data from its users, even if
14 they were not using a Facebook app. That is, Onavo's spyware could obtain information about the user
15 when they were using an entirely different app, such as the YouTube or the Snapchat app. Onavo's
16 spyware also allowed Facebook to exfiltrate user data derived from text messages, including on iMessage,
17 or even from FaceTime calls on iPhones.

18 568. Onavo not only acquired this information, it associated the information with a particular
19 Facebook user. Onavo, therefore, provided Facebook even more certainty as to whether it was correctly
20 matching user actions outside its walled garden with shadow profiles and dossiers that Facebook
21 maintained about its users. Again, Facebook engaged in this conduct in 2017, 2018, and for much of
22 2019.

23 569. This gave Facebook an immense advantage over competitors. While competing apps
24 would have to obtain user data from their own apps, Facebook was able to capture user data from third-
25 party apps in addition to its own. This directly strengthened Facebook's ability to target users for content
26 and advertising, and it gave Facebook a real time view of potential competitive threats as well as the
27 information and time Facebook's own users contributed to those threatening apps. This contributed to
28

FILED UNDER SEAL

and fortified the DTBE, helping maintaining Facebook's Social Advertising monopoly and injuring Plaintiffs and the proposed classes.

IX. THE THREAT BEYOND FACEBOOK'S WALLED GARDEN

570. To maintain its dominant position in Social Advertising, Facebook would have to ensure its ability to granularly target Facebook users. But because those users spent significant time outside of Facebook, including on mobile apps and web applications, Facebook needed to effectively harvest social data from them even when they were not on Facebook. And, to maintain the competitive edge it enjoyed from its DTBE, Facebook would have to extend its ability to target users outside of its walled garden.

A. Facebook Audience Network

571. Facebook announced a new advertising system at the 2014 F8 conference in April of 2014 called the Facebook Audience Network ("FAN"). FAN allowed developers to target both standard banners and custom ad units using Facebook's vast trove of personal data. Advertisers would be able to buy ad space in mobile applications through FAN, and developers could purportedly monetize their apps.

572. As TechCrunch reported ahead of the F8 announcement, FAN would allow advertisers to use Facebook's granular targeting system to advertise in mobile applications:

Facebook will also bring the ad targeting muscle, allowing advertisers to reach people based on biographical and interest data, and likely with cookie-based retargeting, too. Most other ad networks have a limited amount of data regarding who someone is, and that data is often inferred so it's not always accurate. That makes it tougher meaning to show relevant ads that get results and command high rates for publishers. *[sic]*

But Facebook's social network has convinced people to volunteer tons of deep personal information like work history, education, and favorite movies, plus it can see what apps they use and where they are. Since people stay logged into Facebook, FAN can recognize exactly who the viewer is and show them an ad matched to their profile.

573. Part of Facebook's focus was on developers, as they were Facebook's largest mobile ad customer because they sought new users through app installs. FAN would provide new forms of advertising, including early forms of advertising "retargeting"—reengaging with a user after an ad impression or other event. As TechCrunch explained:

FILED UNDER SEAL

1 The ads themselves could promote a range of products. There's sure to be
2 plenty of app install ads, Facebook's current cash cow, as developers are
3 desperate for installs and willing to pay. Mobile app-reengagement ads
4 could also be popular. You might already have Hotel Tonight installed, but
5 have forgotten about it. If Facebook sees you like traveling, and just
6 checked in to a restaurant in Los Angeles, it could show an ad delivered
7 through FAN in another app that re-opens HotelTonight to a \$99 hotel
8 room in the city. Big brands and local businesses might also get in on the
9 action, as Facebook's offline measurement tools can prove that its ads drive
10 in-person sales.

11 574. Facebook was opening up an entirely new class of features—those dependent on tracking
12 users across devices and apps.

13 575. FAN went live in October 2014, and what was launched was significantly broader than
14 what Facebook had announced at F8. FAN was not released as a separate advertising stream. Instead, it
15 was implemented as an extension of Facebook's existing advertising system. This meant that a Facebook
16 Ad, using Facebook's granular targeting systems, could be used to target ads outside of Facebook's
17 properties—directly in third-party, mobile apps.

18 576. TechCrunch covered the new functionality, explaining its significance:

19 Until now, each dollar Facebook earned meant annoying its own users with
20 more ads. This created a natural cap on Facebook's revenue unless it
21 wanted to pester us so much that we stopped visiting. Now it can sit back
22 and cash in on all the targeting data it's collected.

23 577. Facebook had created finely tuned machine-learning systems to target users by, among
24 other things, biographical and interest-based information it had collected about them as they interacted
25 with other Facebook users. Those machine-learning algorithms would now be turned loose outside of
26 Facebook's walled garden, allowing them to granularly target and track Facebook's users even when they
27 were using someone else's mobile application.

28 578. The value of this new functionality was not just the ability to display ads on mobile
applications that Facebook did not control—it also provided Facebook more critical user data, particularly
social data, which its machine-learning algorithms needed as fuel. Facebook would be able to learn more
about its users, including how they interacted with other users and content outside of Facebook,

FILED UNDER SEAL

1 Instagram, or WhatsApp. This made Facebook better at serving both content and advertising to users
2 while on Facebook-controlled apps, reinforcing the DTBE.

3 579. Initially, Facebook's Login product, which it had promoted at F8 2014, was one of the
4 ways Facebook was able to track users across applications. Users who logged into a third-party app using
5 their Facebook login were then tracked by Facebook as they used those apps.

6 580. In May 2016, however, Facebook extended FAN even further, to track Facebook users
7 who were not even logged into Facebook. As Facebook explained in a blog article:

8 Over the coming months we will expand the reach of Facebook-powered
9 advertising on the Audience Network to include people who don't have
10 accounts. To ensure that the ads people see in the apps and websites in the
11 Audience Network are highly relevant, we will use information we receive
12 from third-party sites and apps that use Facebook technology.

13 581. On May 27, 2016, the *Wall Street Journal* reported that the change allowed tracking of
14 users across the Internet, positioning Facebook to compete head-on with Google:

15 To that end, the social network and online advertising company said
16 Thursday it will now help marketers show ads to all users who visit
17 websites and applications in its Audience Network ad network. Previously
18 Facebook only showed ads to members of its social network when they
19 visited those third-party properties.

20 The change is a subtle one, but it could mean Facebook will soon help to
21 sell and place a much larger portion of the video and display ads that appear
22 across the Internet. The change will also intensify competition with
23 Alphabet Inc. subsidiary Google, which dominates the global digital-
24 advertising market, and a wide range of other online ad specialists.

25 582. Facebook now planned to leverage its targeting systems outside its walled garden. It would
26 monitor users who were not logged into Facebook at all, allowing FAN to extend Facebook's edge beyond
27 the Social Advertising Market, which it had dominated by virtue of the DTBE protecting its business.

28 **B. Facebook Acquires Atlas**

583. On December 6, 2012, news broke that Facebook was considering acquiring a company
called Atlas from Microsoft. Atlas was a software company that both served ads and tracked ad
conversions.

FILED UNDER SEAL

1 584. For example, Atlas technology would log when a user viewed an ad that was served to
2 them, and then if they later, for example, purchased a product (that is, the ad “converted”), Atlas
3 technology would allow attribution of the sale to the advertisement.

4 585. Google had paid \$3 billion dollars for its own ad-serving product, DoubleClick, in 2007.
5 Although Atlas lacked the sophistication of DoubleClick—particularly after Google had developed and
6 integrated the DoubleClick software with its own—the purchase of Atlas positioned Facebook to grow
7 and extend its capability to granularly target users with advertising well beyond Facebook’s own
8 properties.

9 586. In Facebook’s hands, however, Atlas and its technology was even more valuable. As
10 Business Insider explained in December 2012:

11 The value of a Facebook-powered/Atlas-supported ad network could be
12 tremendous.

13 Here’s why.

14 Facebook is the only company in the world that has a billion email
15 addresses, home addresses, and phone numbers on file.

16 This asset allows Facebook to do something no other Website can.

17 Facebook can tell marketers whether or not a Facebook user saw, on
18 Facebook.com, an ad for a product before going to the store and buying it.

19 This is possible because retailers often have their shoppers’ phone
20 numbers, home addresses, or email addresses on file. (They buy them from
21 data collection companies.)

22 In the short term, Facebook will use this process to tell marketers exactly
23 how much their sales increased thanks to ads on Facebook.com.

24 587. Acquiring software that could track conversions of Facebook ads outside of Facebook’s
25 walled garden was a powerful extension of Facebook’s targeting apparatus. It closed feedback loops for
26 events that occurred outside of Facebook’s view.

27 588. This ability, however, was about much more. Facebook’s DTBE stems both from the data
28 it harvests from its users and the power of its machine-learning models, which consume that data. As
users spend more time outside of Facebook’s properties, those machine-learning models have less to train

FILED UNDER SEAL

on, reducing the effectiveness of Facebook’s targeting. This in turn reduces engagement within Facebook, and as a result, the value of its targeted advertising. Facebook understood this threat in the early 2010s, with the rise of mobile apps. That is why it was—and remains—vital for Facebook to be able to track its own users when they are not using the core Facebook product, Instagram, or WhatsApp.

589. At its purchase, Atlas already had the necessary functionality, allowing advertisers to plan campaigns, buy ads on sites across the web, and measure their impact. It handled rich media and in-stream video, display ads, and offered APIs for programmatic control.

590. Internally, Facebook saw Atlas as a means to massively increase Facebook’s targeting capabilities. As Amin Zoufonoun, Facebook’s Vice President of Corporate Development, described to Sheryl Sandberg when Facebook was considering the acquisition, it gave Facebook “immediate scale to retarget, provide premium insights, do look-alike modeling, prove and measure efficacy of [Facebook] as a marketing medium, [and] enhance customer audiences and associated revenue.”

591. Most importantly, it gave Facebook the ability to use identity-based targeting through Facebook Identity—Facebook’s unique identifier for Facebook users across all browsers and devices—to serve highly targeted ads. Indeed, Facebook had described the value of Facebook Identity as the ability to “target people across browsers and devices” and to “[a]ctivate offline data to enrich online targeting,” among other features.

592. On February 28, 2013, Facebook acquired Atlas for approximately \$100 million. In its summary of the deal at the time of the transaction, Facebook noted that the transaction was an opportunity to become the “buy-side desktop tool that media planners fire up first thing in the day” and to acquire “a deep installed base of pixels which we can immediately turn on to power conversion tracking and attribution across offerings.”

593. The latter was the most important. By pixels, Facebook was referring to embedded web resources that would automatically pull information from a Facebook server when a user visited a non-Facebook site. Sometimes, this would be done through an invisible, single-pixel image, which would download from a centralized server. When the single-pixel image appearing on a third-party site was

FILED UNDER SEAL

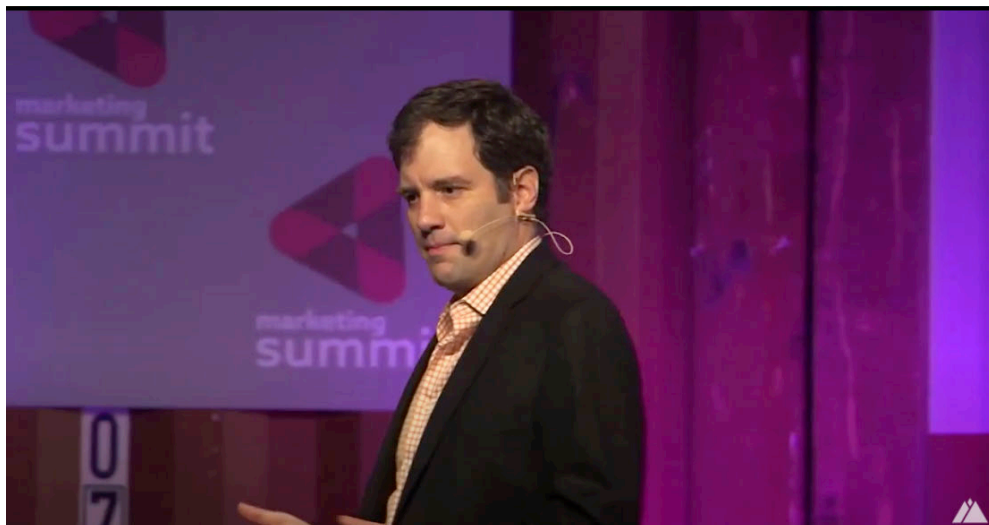
downloaded by a user, Facebook would immediately know and would have the user's browser information, IP address, and device information as a result.

594. On September 29, 2014, Facebook announced through a blog post by Atlas's Managing Director Erik Johnson that Facebook had rebuilt Atlas "from the ground up," meaning that it had integrated it with its Facebook advertising systems. Facebook made the announcement ahead of Advertising Week in New York City.

595. Although Facebook removed the blog post and announcement from its site, *Wired* magazine contemporaneously recounted the focus of the announcement: unlike Google, Facebook would not need Cookies to identify users; it had its own data and targeting systems, which it had trained and honed using user interactions with its own properties:

In an apparent dig at Google, Johnson writes that the method advertisers have traditionally used to track consumers—cookies—is flawed, because consumers are no longer using one device at all times. "Cookies don't work on mobile, are becoming less accurate in demographic targeting and can't easily or accurately measure the customer purchase funnel across browsers and devices or into the offline world," Johnson writes. He offers "people-based marketing," that is, marketing based on Facebook's data, as the solution. It can not only track users between devices, but it can also connect online campaigns to offline sales to determine how effective a given campaign really was.

596. Johnson spoke at the Web Summit 2014 convention on its first day, November 4, 2014 (pictured below).



FILED UNDER SEAL

1 597. The focus of Johnson’s Web Summit talk was identifying users across devices and
2 throughout the Internet by using Facebook’s user targeting technology:

3 If that email address corresponds to an email address you use on Facebook,
4 we can now stitch together ads you’ve seen anywhere on the internet with
5 a purchase you made in a store. Facebook has had this functionality for
6 some time now, but with Atlas, we’re able to take the cross-device, and the
people-based and the offline-to-online story that Facebook has and move
it to the rest of the internet.

7 598. Atlas gave Facebook the ability to leverage and extend its DTBE. Facebook could not only
8 target users as they interacted on Facebook-controlled applications, but when they interacted with other
9 apps and websites. This sharpened Facebook’s own targeting across its properties.

10 **C. Facebook Positions Itself Against Google by Combining Atlas, Audience Network,**
11 **and Other Technology**

12 599. By December 10, 2014, Facebook had acquired several key systems that positioned it to
13 extend its targeting advantage beyond Facebook’s products. In addition to Facebook Atlas and FAN,
14 Facebook had also acquired LiveRail for approximately \$400-500 million.

15 600. LiveRail connected marketers to publishers on web and mobile to target seven billion
16 video ads to visitors per month. It provided for real-time bidding, meaning that it dynamically matched
17 advertisement inventory with bids from marketers to optimize both revenue and effectiveness of that
18 advertising.

19 601. The technology Facebook acquired from LiveRail and Atlas, coupled with FAN, together
20 positioned Facebook to expand its dominance beyond its walled garden (Facebook’s three primary
21 products—Facebook itself, Instagram, and WhatsApp). Facebook’s advertising could reach beyond those
22 apps, tracking users across mobile devices and websites, and using information it gleaned from that
23 tracking to sharpen Facebook’s targeting algorithms within its own products.

24 602. The press likened the combined assets to an “AdTech Voltron,” a cartoon robot that
25 assembled a powerful robot out of smaller pieces:

26 Here’s how the pieces come together.
27
28

FILED UNDER SEAL

Facebook brings its 1.35 billion users and massive engagement with the News Feed where it shows its ads. Because its huge user base stays logged in across web and mobile, it has a unified understanding of people's identities in a way most platforms don't. Facebook's wealth of personal data means it can target ads more accurately. For instance, it says it can target gender with 90 percent accuracy compared to the online ad industry average of 50 percent.

603. The combination of these properties reinforced Facebook's primary form of leverage in the Social Advertising Market—its ability to granularly target users and to do so with significantly more accuracy than any other competing product. By tracking Facebook users both inside and outside of its walled garden, Facebook's targeting system was poised to span the Internet, mobile applications, and Facebook's social applications, including Instagram and WhatsApp.

604. Through a combination of these assets, Facebook was able to create "Lookalike Audiences," a new product announced in March 2013 that allowed Facebook to use its combined tracking information to train its machine learning algorithms to serve ads more likely to "convert" or otherwise result in desired feedback. Facebook could use a tracking pixel on a third-party site to find users within its own applications similar enough to likewise convert on the same site.

605. Facebook itself provides an example on its website:

Say you're an online florist that wants to reach people similar to those that made purchases on your website. Now you can use data from your Facebook pixels (Facebook Conversion Pixel or the Custom Audiences for Websites Pixel) to reach people who are most similar people who previously made purchases on your website.

606. Facebook boasted that e-commerce company Shopify "saw a 2x decrease in cost per lead when using lookalikes of their website visitors."

607. The new method of targeting advertisements meant that Facebook's machine learning was becoming more powerful—capable of self-tuning ad campaigns to maximize their effectiveness. After Facebook's ads had run for a while, they would become more effective without the need for manual user input. Facebook's machine-learning algorithms would optimize not only the ad, but Facebook's revenue. All the while, Facebook's algorithms would harvest more information from the users it tracked, allowing

FILED UNDER SEAL

1 it to further train its machine-learning models. This created a virtuous circle, expanding Facebook's
 2 targeting and trove of social data. The net result was a further strengthening of the DTBE.

3 **D. Shadow Profiles and Identifying Users Outside of Facebook's Apps**

4 608. Facebook's new strategy hinged on identifying its own users outside of Facebook's apps.
 5 By tracking those users outside of Facebook's walled garden, Facebook became better at targeting them
 6 within.

7 609. That is, by becoming better at serving content to users based on their web browsing or
 8 mobile app usage, Facebook could lock users into its own apps, reducing the need for them to leave
 9 Facebook apps while on the internet, which in turn made Facebook ads served to its own users
 10 significantly more effective than other forms of advertising.

11 610. Facebook needed a way to keep track of what users did across mobile applications, its own
 12 applications, and across the web. It did so by maintaining "shadow profiles" on users.

13 611. On April 16, 2018, after significant scrutiny before Congress, Facebook revealed the
 14 sources of the shadow profile data it collects:

15 **When does Facebook get data about people from other websites and**
 16 **apps?**

17 Many websites and apps use Facebook services to make their content and
 18 ads more engaging and relevant. These services include:

- 19 • Social plugins, such as our Like and Share buttons, which make
 20 other sites more social and help you share content on Facebook;
- 21 • Facebook Login, which lets you use your Facebook account to log
 22 into another website or app;
- 23 • Facebook Analytics, which helps websites and apps better
 24 understand how people use their services; and
- 25 • Facebook ads and measurement tools, which enable websites and
 26 apps to show ads from Facebook advertisers, to run their own ads
 27 on Facebook or elsewhere, and to understand the effectiveness of
 28 their ads.

FILED UNDER SEAL

1 When you visit a site or app that uses our services, we receive information
2 even if you're logged out or don't have a Facebook account. This is because
3 other apps and sites don't know who is using Facebook.

4 612. Facebook confirmed its information gathering in its written answers to the United States
5 Senate on June 11, 2018, admitting that Facebook collects extensive data even if a user is not logged into
6 a Facebook account.

7 613. All of this meant that Facebook was uniquely poised to expand and leverage its position
8 in the Social Advertising Market to challenge Google directly in online search and display advertising,
9 where Google had long established a dominant position. As explained in the next section, Facebook never
10 did so. Instead, it made an anticompetitive bargain with Google to preserve the Social Advertising
11 Market—and Facebook's dominance within it.

12 **X. FACEBOOK AND GOOGLE AGREE NOT TO COMPETE AND TO FORTIFY THE**
13 **FACEBOOK-DOMINATED SOCIAL ADVERTISING MARKET**

14 614. Although Facebook was poised to expand its advertising and targeting business beyond
15 its social networking apps, it never meaningfully did so. Instead, as explained below, it made a bargain
16 with Google that would help Facebook sharpen its machine-learning algorithms so that it could maintain
17 its superior ability to target its own users. In exchange, Facebook never challenged Google's dominance
18 outside of the Social Advertising Market.

19 **A. Google's Dominance Over Ad Exchanges and Ad Servers and the Looming**
20 **Facebook Threat**

21 615. As Facebook was taking its first steps outside of its walled garden, Google had already
22 achieved longstanding dominance in a form of advertising that allowed dynamic matching of display ad
23 inventory on websites and apps with marketers seeking to advertise to particular demographics.

24 616. Publishers provided their advertising inventory to Google's Ad Manager ("GAM"), which
25 would then either match that advertising inventory with a purchaser who had made a direct deal for
26 advertising or serve the available inventory to an ad exchange, where marketers bid for the inventory in
27 real time.

28 617. As an example, an online newspaper might have a space available on its site for an
advertisement. It would convey that information to an ad server, which would in turn find a buyer for the

FILED UNDER SEAL

1 space. In some cases, the ad server would send the available space to ad exchanges, which would sell the
2 ad space to the highest bidder.

3 618. By the mid-2010s, Google's ad server had become ubiquitous. Publishers, such as USA
4 Today, ESPN, CBS, Time, Walmart, and Weather.com, used (and still use) GAM. Today, GAM controls
5 over 90 percent of ad inventory from publishers.

6 619. Because most publishers use GAM to sell their inventory, Google serves as a middleman
7 to all the advertising exchanges, where bids from marketers are matched in real time with available
8 advertising inventory.

9 620. In addition to controlling the dominant ad server, Google also runs its own ad exchange,
10 called Google Ad Exchange or "AdX." Google charges an exchange fee for matching purchasers with ad
11 inventory, much of which comes through Google's dominant GAM.

12 621. Google's unique vantage point provides it with the ability not only to control the inventory
13 provided to exchanges, but to win bids against other ad exchanges.

14 622. That is, Google tracks website use through its analytics product. It tracks users on its Gmail
15 product. It tracks users when they use Google News. It even provides free DNS servers, resolving IP
16 addresses and web addresses for users across the internet. Google also has a unique vantage point because
17 of its mobile operating system, Android.

18 623. In recent years, Google's unique tools and properties have made it increasingly better-
19 suited to do what no other advertising exchange can do: identify who the person that visited a publisher's
20 website actually is, *i.e.*, their true, unique identity. Google's ad server and exchange are provided with
21 basic information about the person visiting the publisher's site, such as IP address, device identification
22 information, or browser information. Google's other tools and properties have increasingly positioned it
23 to do make granular identity determinations from this data.

24 624. In short, by the mid-2010s Google's advertising ecosystem was getting better and better
25 at doing something that Facebook had built its entire ad business upon, but could not outside of its own
26 properties—ascertain identity. (And, of course, Google could not, and cannot, serve ads to Facebook's
27 users on its properties.) By late 2016, with the rise of new technology and carefully targeted information
28

FILED UNDER SEAL

1 gathering properties like Android, Google’s ad products threatened to encroach upon Facebook’s
2 identity-focused ad targeting products—and indeed threatened to superset the Social Advertising Market
3 itself by allowing user and identity targeting outside of Facebook’s social network.

4 625. As Google’s capabilities increased, the prospect of a new, highly targeted form of
5 advertising emerged—one that could rival the effectiveness of buying advertising in the Social
6 Advertising Market, where Facebook was dominant and had unrivaled information about its users.

7 626. At the same time, Facebook became increasingly better in the mid-2010s at identifying
8 user identities and demographic information even outside of its own apps. Through Facebook’s series of
9 acquisitions, it was able to target users with its advanced machine-learning, even if the users were not
10 logged into Facebook.

11 627. By 2018, Facebook was a threat to leverage its technology into Google’s territory,
12 including by selling advertising in real-time in mobile applications and on the web. And Google’s rapidly
13 growing prowess in discerning identity was an existential threat to Facebook’s DTBE.

14 628. The two solved their problem by coming to an anticompetitive agreement code-named
15 “Jedi Blue,” as explained later in this Complaint. However, to properly understand the true stakes and
16 context of the once-looming clash of advertising titans, it is critical understand the role of AI and machine
17 learning tools in online advertising—and how these tools were differently wielded by Google and
18 Facebook in the run-up to their 2018 agreement to divide markets.

19 **B. Google’s AI Dominance**

20 629. Unlike Facebook, Google spent the 2010s becoming preeminent in machine learning and
21 artificial intelligence. For example, Google acquired groundbreaking AI technology when it purchased
22 UK-based DeepMind in January 2014 for more than \$500 million. And Google has leveraged this and
23 other bleeding-edge machine learning technology throughout its entire ecosystem ever since.

24 630. Google’s machine-learning dominance has allowed it to leverage its large cross-section of
25 user data across the Internet and mobile applications in increasingly powerful ways. For example, on
26 December 14, 2016, Google announced that it had used DeepMind technology to make recommendations
27
28

FILED UNDER SEAL

1 on its Google Play Store—Google’s mobile app store for Android devices. Google explained the problem
2 and its AI-based solution on its AI blog:

3 Providing useful and relevant app recommendations to visitors of the
4 Google Play Apps Store is a key goal of our apps discovery team. An
5 understanding of the topics associated with an app, however, is only one
6 part of creating a system that best serves the user. In order to create a better
7 overall experience, one must also take into account the tastes of the user
8 and provide personalized recommendations. If one didn’t, the “You might
9 also like” recommendation would look the same for everyone.

10 Discovering these nuances requires both an understanding what an app
11 does, and also the context of the app with respect to the user. For example,
12 to an avid sci-fi gamer, similar game recommendations maybe of interest,
13 but if a user installs a fitness app, recommending a health recipe app may
14 be more relevant than five more fitness apps. As users may be more
15 interested in downloading an app or game that complements one they
16 already have installed, we provide recommendations based on app
17 relatedness with each other (“You might also like”), in addition to
18 providing recommendations based on the topic associates with an app
19 (“Similar apps”).

20 One particularly strong contextual signal is app relatedness, based on
21 previous installs and search query clicks. As an example, a user who has
22 searched for and plays a lot of graphics-heavy games likely has a
23 preference for apps which are also graphically intensive rather than apps
24 with simpler graphics. So, when this user installs a car racing game, the
25 “You might also like” suggestions includes apps which relate to the “seed”
26 app (because they are graphically intense racing games) ranked higher than
27 racing apps with simpler graphics. This allows for a finer level of
28 personalization where the characteristics of the apps are matches with the
preferences of the user.

631. Google thus tackled a problem Facebook had solved socially (with actual social data), but
did so in a different way—by using complex machine learning that did not require social signals to make
social evaluations and recommendations. Rather than collecting actual friend recommendations and
activity, Google used machine learning—*i.e.*, deep neural network models—to study a user’s decisions
and preferences, then identified that other apps that might interested that user.

632. Facebook, on the other hand, had monetized app installs for years—Facebook’s “cash
cow”—by using its social targeting systems to traverse its network and coax other users to install apps

FILED UNDER SEAL

1 using social connections. Facebook used social data, data about its users' interactions within its social
2 network, to devise and train machine-learning algorithms that would make predictions about who would
3 be interested in installing an app.

4 633. It was this "recommendation engine" technology that was at the center of Zuckerberg's
5 concerns about Tinder during Facebook's early 2010s API scheme. Indeed, in January 2014, Zuckerberg
6 was concerned that "recommendations seems like something that should be right up our alley," but was
7 "something we're not very good at." He found Tinder's growth "alarming" because its recommendation
8 engine was "built completely on Facebook data" and was "much better than anything we've built for
9 recommendations using the same corpus."

10 634. But as Facebook sought to expand its machine-learning capability outside of its walled
11 garden, it faced a Google that was far ahead of it in the field of artificial intelligence and machine learning.
12 This meant that Google was better at identifying users, and if left unchecked, would be better at targeting
13 Facebook's own users throughout the Internet, including on mobile applications.

14 **C. The Rise of Header Bidding and Facebook's Threat to Compete with Google**

15 635. By 2016, a competitive collision between Facebook and Google looked imminent.
16 Facebook was well positioned to move into the ad exchange business, and Google was poised to break
17 Facebook's dominance over granular, identity-based ad targeting, including within long-siloed social
18 networks such as Facebook, Instagram, and WhatsApp.

19 636. The threat of competition heightened in 2015 and 2016 when publishers began to adopt a
20 practice called "header bidding." Header bidding routed ad inventory to multiple neutral exchanges each
21 time a user visited a web page in order to return the highest bid for the inventory.

22 637. That is, publishers could send a standardized header to several exchanges, which included
23 information about the advertising slot and the visiting user, and bidders on the exchanges could within
24 milliseconds place bids for that advertising slot.

25 638. The new header-bidding technology threatened to cut Google out of the picture. Not only
26 did header bidding undermine Google's ad server, which had routed advertisements to the exchanges, it
27
28

FILED UNDER SEAL

1 also eroded Google's ability to front-run third-party ad exchanges by giving its own ad exchange an
2 information advantage.

3 639. Google created its own alternative to header bidding, called Open Bidding, which among
4 other things, allowed Google an advantage over other exchanges, including by charging a penalty fee
5 when an ad was sold on a non-Google exchange.

6 640. Google aggressively sought to quell the threat of header bidding, but the threat became
7 existential when Facebook threatened to adopt header bidding. In March 2017, Facebook publicly
8 announced it would support header bidding, including in connection with FAN. At that time, when
9 bidding into Google's ad server, networks such as Facebook's FAN had to bid into exchanges and pay
10 exchange fees. By adopting header bidding, Facebook would let web publishers, mobile app publishers,
11 and advertisers avoid Google's exchange fees altogether. They could simply header bid to the exchanges,
12 including through Facebook's valuable FAN.

13 641. This was viewed as a direct attack on Google's supremacy. Ad Age reported as much on
14 March 22, 2017:

15 Facebook just executed what might best be described as a digital
16 advertising coup against rival Google and its DoubleClick empire.

17 The social media power said Wednesday that it's bringing advertiser
18 demand from its Audience Network to mobile web publishers that use
header bidding.

19 Mobile publishers have been able to tap demand from Facebook Audience
20 Network until now so long as they didn't use header bidding technology, a
21 system that allows them to take bids from multiple buyer pools all at once.
But if they wanted to capitalize on header bidding, they had to forgo any
demand in FAN.

22 Now publishers that used header bidding and want to tap advertisers
23 coming through FAN can do so through Facebook technology partners
24 Index Exchange, Sonobi, Amazon Publisher Services, AppNexus,
Media.net and Sortable. They can also access FAN through open-source
25 solutions PreBid and PubFood, the company said.

26 642. As Ad Age observed, the move meant that Facebook's preeminent, identity-based
27 targeting system could now be leveraged across the internet:
28

FILED UNDER SEAL

Publishers like the Washington Post, Daily Mail and Forbes have been quietly working with Facebook to introduce the offering, which gives them the ability to plug into FAN and receive ads bought through Facebook's sophisticated data and targeting technology.

643. Facebook's move had been part of a long-term strategy to draw in Google. Facebook's gambit worked, and Google reached out to Facebook to broker a deal.

D. Google Agrees to Help Facebook Identify Facebook's Own Users Outside of Its Walled Garden, and Facebook Backs Off of Programmatic and Exchange-Trade Advertising

644. Within months of Facebook's official header bidding announcement, Google and Facebook began formal negotiations. By August 2018, the companies were in heated negotiations, with each company internally evaluating contingencies and strategies if no deal could be reached.

645. In September 2018, the companies finally reached an agreement—an anticompetitive one. The agreement was code-named Jedi Blue.

646. Facebook agreed to back off its support of header bidding, leaving Google's dominant position over exchange-based advertising intact.

647. In exchange, Google agreed to give Facebook what it needed—a means to track its own users when outside of Facebook-controlled apps.

648. As part of the agreement, Facebook would pay Google a 5 to 10% transaction fee and would be locked into spending \$500 million annually on Google's exchange-based systems.

649. Facebook, in return, would keep its control over the Social Advertising Market. In fact, because of the agreement, Facebook was able to ensure that Google's targeting would not target Facebook's users, solidifying Facebook's preeminence over advertising to users on its social networks. In short, Facebook's agreement with Google shored up Facebook's DTBE within its walled garden at a time when the very existence of a differentiated, Facebook-dominated Social Advertising Market was under threat from advancements in programmatic advertising and tracking technology.

650. As reported by the *Wall Street Journal*, Google provided Facebook a series of concessions to Facebook as part of Jedi Blue that ensured this. For example:

FILED UNDER SEAL

- Google would help Facebook recognize mobile and web users, particularly Facebook’s own users as they used websites and third-party applications.
- Facebook would receive the right to show ads to 90% of the users it recognized as its own.
- Facebook would receive a 300 millisecond “timeout” to recognize its users and bid. Other participants would receive a shorter, 160 millisecond timeout.

651. The threat of Facebook leveraging its targeting systems in Google’s space was quelled—by agreement. In exchange, Google propped up the Social Advertising Market. Because Facebook could identify its own users outside of its apps, Facebook could maintain a price premium when it sold advertisements to those users. Facebook also received preference over those users, meaning bidders on other exchanges would only get the remaining 10% of inventory, and even then, would have half the time Facebook had to bid on that inventory.

652. Google handed Facebook control over advertising targeting Facebook users and users of other Facebook-controlled apps. This meant that Facebook became the most valuable means of reaching these users, including while using third-party apps or websites.

653. Without the agreement, Google’s machine-learning and AI dominance would allow it to identify users, including Facebook’s own users, and target them, eventually based on granular criteria. This would erode the DTBE protecting Facebook’s Social Advertising Market and reduce the price premium Facebook could charge (and did charge) for reaching its users.

654. Because of Jedi Blue, Facebook’s users remained uniquely Facebook’s to advertise to. As a result, advertisers had to pay Facebook (at a premium) to advertise to those users using granular targeting, including demographic-based targeting. By reason of the Jedi Blue agreement, no fungible level of targeted advertising could (or did) emerge that could rival Facebook’s ad products for its walled garden users.

655. The agreement also neutralized (or at least substantially delayed) the AI and machine-learning threat posed by Google. Although Google was able to determine the identity of users based on publisher-provided information and its own data collected throughout the Internet, it would not leverage that data to poach advertising sales from Facebook. Rather, Facebook would receive priority over

FILED UNDER SEAL

1 advertisements to its own identified users—and would receive Google’s help to identify those users.
2 Instead of turning its technology against Facebook, Google used it to bolster Facebook’s dominant
3 position in the Social Advertising Market.

4 656. Put simply, Google and Facebook agreed to divide and segment markets, allowing
5 Facebook to continue charging a significant price premium for its targeted advertising sold in the Social
6 Advertising Market. The agreement also staved off competition that threatened Google’s control over
7 exchange-traded advertising throughout the Internet. Both competitors benefited. Competition did not.

8 **XI. FACEBOOK ANTICOMPETITIVELY INTEGRATES THE BACKENDS OF**
9 **INSTAGRAM, WHATSAPP, MESSENGER, AND ITS CORE FACEBOOK PRODUCT**

10 657. Facebook had entered into an agreement with Google to identify Facebook users as they
11 interacted with websites and apps outside of Facebook’s walled garden. With its resources freed up,
12 Facebook turned inward to finally seal off any competition in the Social Advertising Market, significantly
13 and irreversibly strengthening the DTBE.

14 658. Facebook had for years operated its WhatsApp and Instagram applications as separate
15 businesses. Indeed, Facebook pledged to regulators to keep the companies and their massive data stores
16 separate. By the end of 2018, shortly after Facebook entered into the Jedi Blue agreement with rival
17 Google, Facebook abruptly began considering the integration of the backend software of Facebook,
18 Messenger, WhatsApp, and Instagram, which would create the largest aggregation of social data in the
19 world. The purpose of this integration was not (legitimately) technical; rather, the entire plan was an
20 attempt to irreversibly commingle Facebook’s various data sources, products, and models so that
21 regulators could not eventually break up, divest, or otherwise cleanly enjoin or monitor the company after
22 a year of growing, worldwide concern about Facebook’s data practices and market power.

23 659. However, regulatory scrutiny heated up even faster than Zuckerberg had anticipated. By
24 March 2019—just months after Zuckerberg first decided to integrate Facebook’s back end, and as the
25 company was just starting to grapple with the massive technical and product resources the integration
26 would require—numerous U.S. Senators, including Presidential candidate Elizabeth Warren, had
27 expressly and publicly called for the company to be broken up.
28

FILED UNDER SEAL

1 660. Zuckerberg and Facebook scrambled to proceed with the backend integration, specifically
2 discussing Warren and other regulators’ concerns. In order to distract and delay regulators, Zuckerberg
3 and Facebook’s Vice President of Global Affairs, Nick Clegg, internally prepared and then aggressively
4 promulgated a smokescreen—a pretextual claim that the integration was in fact a push to implement end-
5 to-end encryption across Facebook’s apps. In reality, end-to-end encryption was a solved problem—it
6 had already been successfully implemented by Facebook in WhatsApp product years earlier—and was
7 wholly tangential to Facebook’s back-end integration plans. However, the smokescreen worked:
8 regulators and the media extensively argued about the propriety of end-to-end encryption (which
9 implicates serious law enforcement concerns, among other policy issues) in Facebook’s products, while
10 the integration itself was all but forgotten.

11 661. This was a problem, because Facebook’s back-end integration was not only a means of
12 sealing of competition and strengthening the DTBE, but also a means to prevent regulators from divesting
13 Facebook of WhatsApp and Instagram—or otherwise disaggregating the company’s distinct products and
14 data sources.

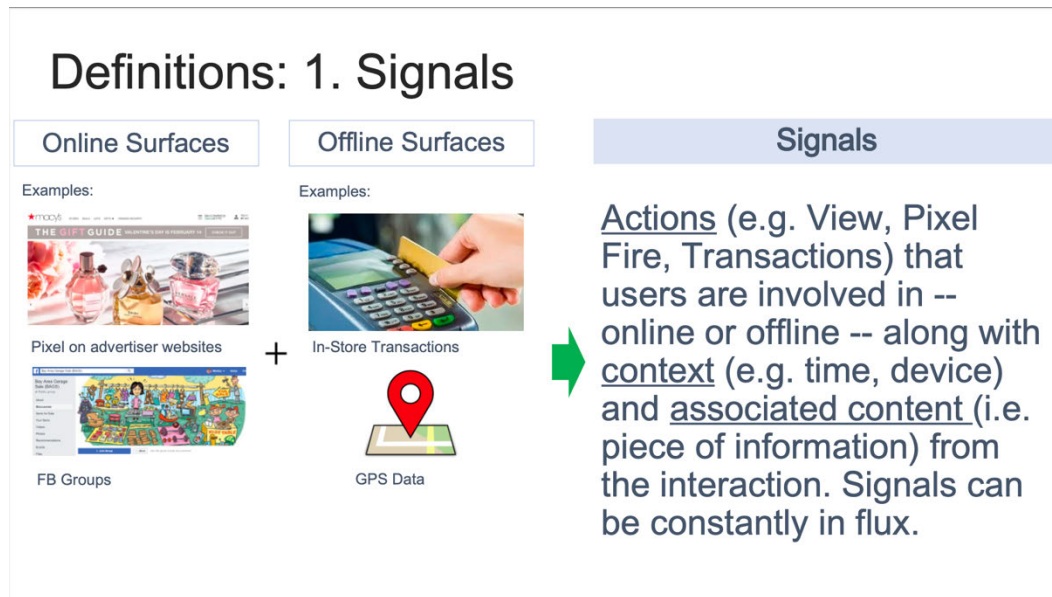
15 662. Facebook’s back-end integration lacked any legitimate technical justification, but was
16 instead solely a means to prevent the regulatory breakup of Facebook, Instagram, and WhatsApp and to
17 cement Facebook’s dominance over the Social Advertising Market.

18 **A. Facebook’s Social Data Refinement, Signal Extraction, Data Structuring, and**
19 **Feature Creation Process.**

20 663. Facebook’s social advertising business required extraction of social data from users as
21 they interact with Facebook’s products and services. Facebook refines this social data into “signals”:
22 inputs to its ML and AI models that could be used to derive a user’s intent and to predict user behavior,
23 including their response to advertising or content.

FILED UNDER SEAL

664. As an internal Facebook presentation explained, “signals” are actions such as a user viewing content or a pixel on a third-party site firing. A signal can also be the context for an event that occurs either online or offline, such as the time something occurs, or the device used to access something. The associated content accessed by the user is also a signal. (See PALM-006784826, at slide 26.)



(*Id.*)

665. Additionally, Facebook determines a user’s identity based on interactions and social data it receives through its properties. Although signals from a user change, or as Facebook puts it, are “constantly in flux” (*id.*), identity is for the most part fixed. It consists of a user’s key attributes, such as the user’s name, phone number, or list of contacts. Facebook defined “identity” in an internal presentation as follows:

Definitions: 2. FB identity

Connection of entities, with each entity representing a person with attributes (such as name, demographic, contact), that rarely change (relative to pixels which are a constant flow of data) and often, but not always, is inputted by the user (vs. inferred)

(PALM-006784826, at slide 27.)

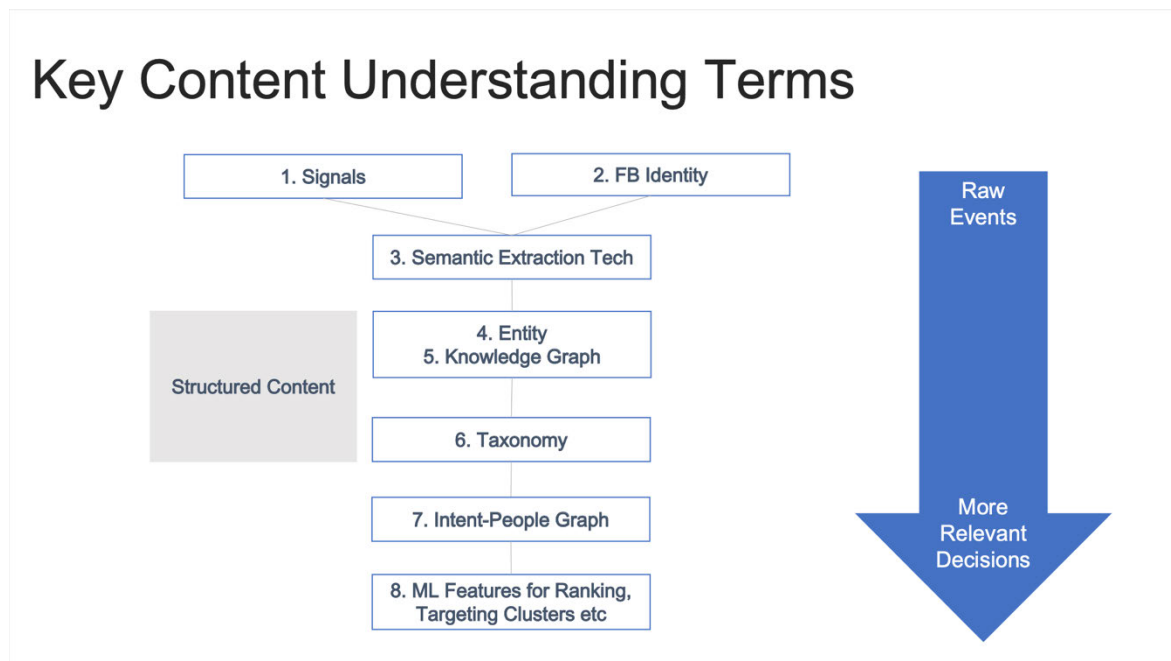
666. For Facebook, “identity” was always baseline information Facebook’s own users provided when they signed up for an account and interacted with Facebook’s products. Within Facebook’s walled

FILED UNDER SEAL

garden, identity was a tractable problem—sometimes even a trivial one. A user that logs into Facebook or logs into an app using Facebook’s “Login” product would essentially self-identify. Facebook could then pull that user’s profile and append streams of signals to it so that predictions or inferences could be made about the user.

667. Outside of Facebook’s walled garden, identity was significantly more difficult, which is why Facebook relied on Google after its “Jedi Blue” agreement to identify Facebook’s own users across the World Wide Web and in mobile apps.

668. Facebook uses identity and signal data together to extract and refine data so that it can be used by Facebook’s ML and AI. This transforms the data that Facebook collects at the top of the purchase “funnel” (further away from the user purchase or conversion) into predictions about a user’s intent. Facebook internally provided a diagram of this refining process:



(PALM-006784826, at slide 25.)

669. The next step in Facebook’s process is to analyze the underlying data from the signals—namely, the content the user has interacted with—such that the content can be turned into quantitative or structured data. In other words, Facebook next makes sense of the content that the user has viewed,

FILED UNDER SEAL

shared, liked, or even lingered on while browsing. Facebook calls this process “semantic extraction” and maintains software tools to perform that extraction:

Definitions: 3. Semantic Extraction Tech

Tools used together information from online and offline surfaces (e.g. web crawler, GPS, Lumos data collection tool), extract semantic understanding from content (e.g., image processors like x-ray and optical character recognition), and map content in a structured way.

(PALM-006784826, at slide 28.)

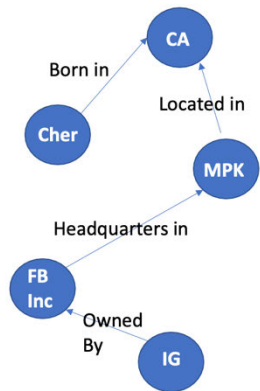
670. Facebook next structures the data it has extracted by creating “entities,” then mapping the entities together. As the internal Facebook presentation explains, an entity can be anything in the real world that has descriptive attributes:

Definitions: 4. Entity

Real-world things (e.g., celebrities, places, products, concepts) that have descriptive attributes (e.g., brand, version, price). Represented by FB object (e.g. Page or keyword) with properties.

(PALM-006784826, at slide 29.)

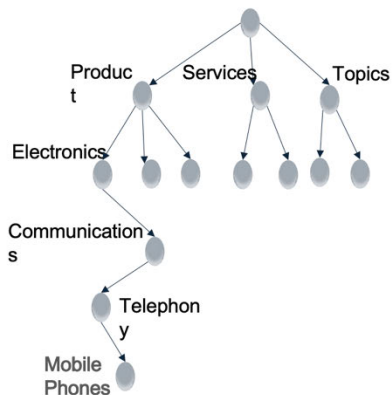
671. Facebook prepares a “knowledge graph” that maps various entities together, creating structured data about the relationships among entities. This allows an ML or AI system to traverse the graph to determine relationships between or among things. Facebook describes the “Knowledge Graph” as a “relationship map[]” that describes entities using the “attributes that connect them.” (PALM-006784826, at slide 29.)

FILED UNDER SEAL**Definitions: 5. Knowledge Graph**

Entity ↔ Entity relationship mapping with attributes that connect them. The connections (or edges) are explicitly named. E.g. Menlo Park “located in” California, outdoor enthusiast “interest in” hiking boots. The Knowledge Graph aims to represent the real world.

(Id.)

672. Facebook also structures the data it receives into a “taxonomy”—a hierarchical structure, like a tree of concepts / entities. This essentially categorizes the data. As Facebook explained in an internal presentation:

Definitions: 6. Taxonomy

Human-defined categories in a tree-like structure. Each node is an aggregation of nodes below. The leaf nodes cover all entities

(PALM-006784826, at slide 30.)

FILED UNDER SEAL

1 673. From there, Facebook maps a user to entities. This may include predictions about a user's
2 "intent"—such as whether they are likely to buy a particular good or service. This mapping is one of the
3 essential precursor inputs to Facebook's ML and AI models. In the same internal presentation, Facebook
4 defined the "Intent-People Graph" as follows:

5 Mapping of people's (accounts) interactions with entities. More advanced
6 versions can map a prediction for intent to people (accounts) e.g. "in the
7 market for hiking boots". Intent will be a function of ordering of events,
8 actions against the entities, and spatial components (e.g., how long ago was
9 action)

10 (PALM-006784826, at slide 32.)

11 674. Once structuring has occurred, Facebook refines the signals it obtains into "features" using
12 ML and AI. These features are used in conjunction with ML and AI models to make predictions about
13 the user. Facebook's models generally provide rankings to match users with advertising or with
14 recommended content. As Facebook explains:

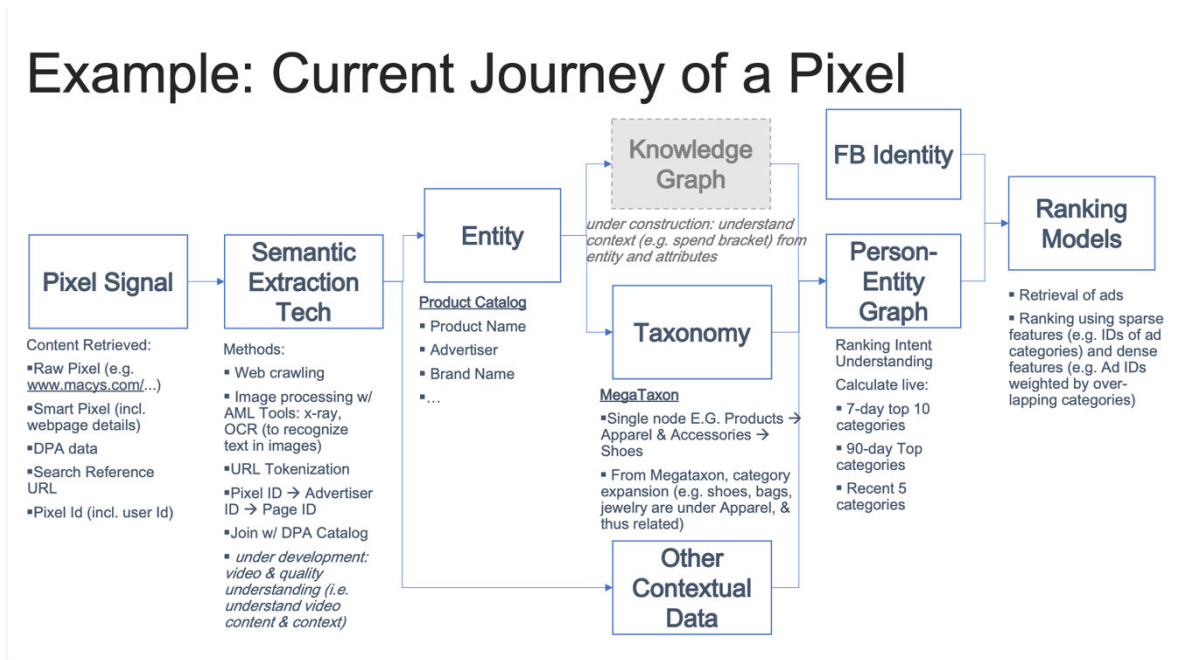
15 **Definitions: 8. Ranking Models**

16 ML models, features, and utility functions used to leverage Person-Entity
17 Graphs for a specific use-case (e.g. recommendations for ads/search/feed
18 stories/etc., targeting in ads, transparency & control tools)

19 (PALM-006784826, at slide 33.)

FILED UNDER SEAL

675. Facebook's internal presentation provided an example of this data refinement pipeline in the context of a Facebook Pixel that fires on a third-party site or app:



(PALM-006784826.)

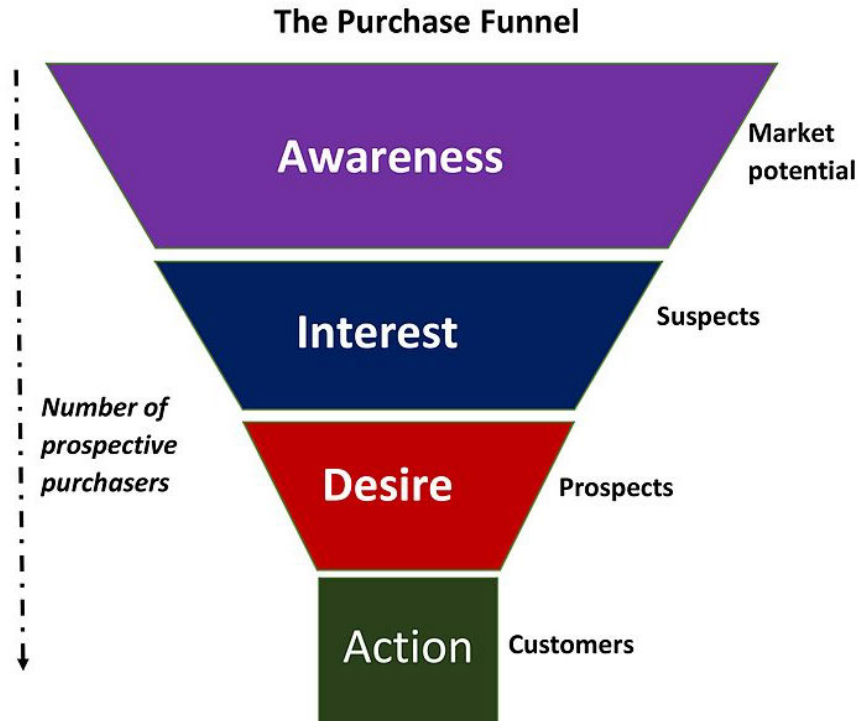
676. As Facebook explained, its ML and AI models facilitate the retrieval of ads and then the ranking of users and ads with respect to each other. (*See id.*)

677. For years, Facebook maintained user “intent” information on what it called the “Intent Platform.” This allowed Facebook, Instagram, and WhatsApp to build AI and ML models based on user intent information collected and refined from social data.

678. Moreover, Facebook internally matched user profiles across its applications. Beginning from the acquisitions of WhatsApp and Instagram, Facebook was able to determine the identity of users across its apps.

FILED UNDER SEAL**B. Facebook and Identity**

679. Facebook occupies a different position in what it refers to as the advertisement “funnel” than other Internet advertisers. An advertising or purchase funnel is a way to describe the narrowing number of advertising targets remaining as one sorts for likelihood to act—or to “convert.”



680. Under this model, the further one gets from the point of action or conversion, the more prospective purchasers there are. Far fewer of those prospective purchasers will ever make a purchase than those that have an interest in, or even a desire to purchase, the product.

681. Facebook, unlike search-engine Google, collects its data higher up the funnel—that is, further away from the point of conversion. This is because when a user interacts with a search engine, she essentially communicates what she is looking for to the search bar.

682. As an internal Facebook presentation explained:

FB Inc.’s position of strength today is at the top of the consumer journey (discovery, navigation, inquiry). *More specifically we own large portions of the top of the funnel. (e.g. FB app, IG, Messenger, WA, etc.),* and also some “commerce enablement” tools focused on what we own (e.g., our business facing tools for the FB family). The broader “commerce enablement infrastructure” we are outlining here goes beyond our internally focused solutions and into market-wide solutions (e.g.,

FILED UNDER SEAL

1 SEO/SEM on Google, integration into Amazon Marketplace, etc.), down
2 funnel in the consumer journey (e.g. fulfillment, payment platform across
3 channels, etc.) and operations (that are not directly part of the funnel).

4 (PALM-006782242, at 44 (emphasis added).)

5 683. Facebook understood that the intent data enjoyed by search or e-commerce sites was a
6 more direct form of user intent data than its stock in trade. Facebook, on the other hand, derives and infers
7 user intent from the social data it gathers.

8 684. The bulk of Facebook's revenue has historically come from the top of the funnel (e.g.,
9 from follows, swipes, and clicks in its products), while its lower funnel revenue has come from "offsite"
10 signals, meaning after a Facebook user clicks an ad and is directed to a third-party site. Facebook derives
11 those "offsite" signals from means such as its Pixel or from the use of its Login product with a third-party
12 app or website.

13 685. By the last quarter of 2018, Facebook had all but abandoned "offsite" signals such as user
14 activity entirely outside of its walled garden (*i.e.*, on the open Internet or in the physical world). Facebook
15 had handed off its targeting in that space to Google by agreement, therefore doubling down on targeting
16 its own users inside its walled garden.

17 686. With Google protecting Facebook's down-funnel position by identifying Facebook users
18 on the open Internet, Facebook could focus its efforts towards the top of the funnel, where Facebook had
19 to first identify users, then, using user attributes and social data, target them with advertising and content.

20 687. Facebook has long excelled toward the top of the funnel. This is where Facebook,
21 Instagram, and WhatsApp provide the most social data, which is used to infer user intent and to target
22 advertising or content. By the end of 2018, Facebook's business model relied on social data from the top
23 of the funnel (and what Facebook got from Google), and its WhatsApp and Instagram products greatly
24 augmented Facebook's core products, such as Messenger and Facebook Blue.

25 688. At the same time, Facebook had retreated from expending resources to gather offsite
26 signals by cutting a deal with Google. This meant that by the beginning of 2019, Facebook could turn its
27 attention entirely toward its own ability to maintain dominance over the top of the funnel. If Facebook
28 lost control over surveillance-based advertising targeting—ad targeting based on a user's observed

FILED UNDER SEAL

1 behavior toward the top of the funnel—it risked losing the DTBE protecting its business and, accordingly,
2 its Social Advertising monopoly.

3 689. In order to further protect its DTBE and maintain its Social Advertising market power
4 after the Jedi Blue deal, Facebook turned in 2019 to an anticompetitive product integration.

5 **C. Facebook Begins a Rapid Back-End Integration Effort in Response to Antitrust**
6 **Scrutiny**

7 690. At the time of the Instagram and WhatsApp acquisitions, Facebook had promised
8 regulators that it would operate Instagram and WhatsApp as separate businesses from its core
9 applications, Facebook and Messenger.

10 691. For example, Facebook had represented to the European Commission’s competition
11 regulator that it was unable to match user profiles across WhatsApp and Instagram. The EC regulator
12 relied on those statements as part of its 2014 merger review process.

13 692. On May 17, 2017, the EC regulator fined Facebook €110 million and explained its reasons
14 for the fine in the following press release:

15 The European Commission has fined Facebook €110 million for providing
16 incorrect or misleading information during the Commission’s 2014
17 investigation under the EU Merger Regulation of Facebook’s acquisition
18 of WhatsApp

19 When Facebook noticed the acquisition of WhatsApp in 2014, it informed
20 the Commission that it would be unable to establish reliable automated
21 matching between Facebook’s users’ accounts and WhatsApp users’
22 accounts. It stated this both in the notification form and in a reply to a
23 request for information from the Commission. However, in August 2016,
24 WhatsApp announced updates to its terms of service and privacy policy,
25 including the possibility of linking WhatsApp users’ phone numbers with
26 Facebook users’ identities.

27 On December 2016, the Commission addressed a Statement of Objections
28 to Facebook detailing its concerns.

The commission has found that, contrary to Facebook’s statements in the
2014 merger review process, the technical possibility of automatically
matching Facebook and WhatsApp users’ identities already existed in
2014, and that Facebook staff were aware of such a possibility.

FILED UNDER SEAL

693. Facebook had lied to regulators to push its acquisitions through anticompetition review by EC regulators. Facebook was always able to match user identities.

694. In fact, Facebook had built a dominant position higher up the funnel by positively identifying users across Facebook, Messenger, WhatsApp, and Instagram. Match rates across these apps were extremely high, particularly relative to offsite match rates to user profiles.

695. Facebook had begun building matching infrastructure almost immediately after it completed both acquisitions and after it had eliminated competition from its platform in April 2015.

696. By 2018, Facebook's practice of matching users across applications had infuriated the founders of Instagram and WhatsApp. In March 2018, WhatsApp's founder Brian Acton quit in protest, stating on Twitter: "It is time. #deletefacebook."



697. Zuckerberg had reneged on his promise to limit the monetization of WhatsApp for five years, and had almost immediately begun to monetize WhatsApp by matching WhatsApp's massive user base with Facebook's existing user profiles in order to target advertising and to collect social data.

698. Acton left behind \$850 million in stock when he quit in protest.

699. WhatsApp's other co-founder, Jan Koum, left in April of 2018. Likewise, Instagram's founders Kevin Systrom and Mike Krieger followed suit shortly after, resigning from Facebook in the Fall of 2018.

700. By the end of 2018, Facebook's dominance over top and mid-funnel social data collection and advertising targeting was well established. Facebook's probabilistic matching system did the job and did the job well. Facebook was extracting massive amounts of revenue from the signals and social data it collected from WhatsApp, Instagram, and Facebook with the infrastructure and matching systems in use at that time.

FILED UNDER SEAL**D. The Call to Break Up Facebook, WhatsApp, and Instagram**

701. On March 20, 2018, the Washington Post reported that the Federal Trade Commission had opened an investigation after Facebook's infamous Cambridge Analytica scandal. In the run-up to the 2016 United States Presidential election, Facebook had allowed Cambridge Analytica to pull massive amounts of user information through Facebook's APIs, affecting tens of millions of Facebook's users. The scandal was surprising, as Facebook had been telling developers and the public that it was no longer allowing third-party apps to access to a user's friends and feed information. The FTC immediately began looking into whether Facebook had violated its 2011 consent decree with the agency.

702. On April 10, 2018, Mark Zuckerberg was called to testify before the United States Senate. Senators' questions pointedly turned to Facebook's monopoly position, particularly during questioning by Senator Lindsey Graham of South Carolina. Graham repeatedly questioned Zuckerberg about Facebook's competitors, and directly asked him if the company had a monopoly.

703. By the end of 2018, there was widespread public sentiment, including in Washington D.C., that Facebook had become an anticompetitive monopolist. Several United States Senators introduced measures to reduce Facebook's market power, including by proposing modifications to statutory provisions under the Communications Decency Act that have been interpreted to provide Facebook with broad legal immunities that many other companies did not and do not enjoy. As a September 5, 2018, article in The Verge recounted:

In some ways, Facebook is the most urgent case. It's inescapable, opaque, and wields immense power over the fundamental functions of our society. More than any other tech giant, Facebook's power feels like an immediate threat and the most plausible first target for congressional action. Sen. Mark Warner (D-VA) has already laid out 20 different measures that would rein in Facebook and other tech giants, ranging from GDPR-style data portability requirements to more carveouts of Section 230.

But while Warner's measures focus on nudging Facebook toward more responsible behavior, a growing number of critics see the problem as Facebook itself. It may be that a social network with more than 2 billion users is simply too big to be managed responsibly, and no amount of moderators or regulators will be able to meaningfully rein the company in. For those critics, social networks are a natural monopoly, and no amount

FILED UNDER SEAL

of portability requirements will ever produce a meaningful competitor to Facebook or a meaningful check on its power.

If that's true, *a classical antitrust breakup (as some have suggested) would seem like the only option.*

(emphasis added).

704. Cries to break up Facebook were becoming more common. Professor Tim Wu, known for his work on “net neutrality”—in fact, for coining the phrase—had called for Facebook’s breakup. His focus was Instagram and WhatsApp. A September 2018 article in The Verge explained Wu’s position:

I think if you took a hard look at the acquisition of WhatsApp and Instagram, the argument that the effects of those acquisitions have been anticompetitive would be easy to prove for a number of reasons, says Wu. And breaking up the company wouldn’t be hard, he says.

705. On March 8, 2019, Senator Elizabeth Warren—then running for President of the United States—directly called for the breakup of Facebook. Warren’s focus was on the Instagram and WhatsApp acquisitions. As Warren stated in a blog post, she believed several big tech mergers should be unwound, including Facebook’s WhatsApp and Instagram acquisitions:

Current antitrust laws empower federal regulators to break up mergers that reduce competition. I will appoint regulators who are committed to using existing tools to unwind anti-competitive mergers, including:

- Amazon: Whole Foods; Zappos
- Facebook: WhatsApp; Instagram
- Google: Waze; Nest; DoubleClick

Unwinding these mergers will promote healthy competition in the market—which will put pressure on big tech companies to be more responsive to user concerns, including about privacy.

E. Zuckerberg Decides to Integrate Facebook, Instagram, and WhatsApp, and Plans a Pretextual Smokescreen to Avoid Backlash from Antitrust Regulators

706. By the beginning of 2019, as calls to break up Facebook reached a fever pitch, Zuckerberg had internally ordered the integration of the backends of WhatsApp, Instagram, and Facebook. Zuckerberg’s mandate would set in motion an extensive, largely irreversible process that required

FILED UNDER SEAL

1 thousands of Facebook engineers and other employees to reconfigure WhatsApp, Instagram, and
2 Facebook, as well as Facebook's ad and content targeting infrastructure.

3 707. As Zuckerberg quietly pushed the process forward, Elizabeth Warren's call to break up
4 Facebook got Zuckerberg's and other C-suite executives' immediate attention. On March 8, 2019, the
5 day of Warren's blog post about breaking up Facebook, Zuckerberg wrote to Sheryl Sandberg, Facebook
6 VP for Global Affairs and Communication Nick Clegg, Facebook VP for Global Communications,
7 Marketing, and Public Policy Elliot Schrage, and Facebook VP for Communications Caryn Marooney
8 (previously the founder and CEO of the OutCast Agency):

9 I'm sure you've all seen the news today that Warren is making antitrust
10 and breaking up the tech companies a centerpiece of her campaign. I worry
11 we're miscalibrated on the sensitivity and severity of these issues.

(PALM-006205414, at 15.)

12 708. Zuckerberg was rightly worried: his recently-deployed plan to integrate WhatsApp,
13 Instagram, Facebook, and Messenger was a giant technological and strategic undertaking specifically
14 designed to prevent divestiture a few years down the road, in case antitrust scrutiny on Facebook
15 increased and an agency such as the FTC (or even the Department of Justice) sought an injunction to
16 break up the company. But the plan would take months, even years, and require the work of thousands of
17 Facebook engineers and other personnel—and it had to look like something other than an anti-regulatory
18 measure.

19 709. Warren's public statement was sure to place the public (and perhaps, regulatory) eye on
20 Zuckerberg's incipient integration plan. And under scrutiny, the truth about Facebook's hastily-planned
21 back-end integration—that it had no legitimate technical justification besides making Facebook more
22 resistant to government-ordered divestiture or similar injunctive relief—would likely come out sooner
23 rather than later.

24 710. Zuckerberg needed a smokescreen to hide the true purpose and intent of the integration.
25 So he went immediately to his top public relations executives—Sandberg, Clegg, Schrage, and
26 Marooney—and the brainstorming session did not disappoint.

FILED UNDER SEAL

711. The answer, familiar to anyone at Facebook who had weathered the earlier Platform scheme, was to claim that the just-announced back-end integration of WhatsApp, Instagram, Facebook, and Messenger was to protect users' privacy. And the person who thought of this idea—and clearly framed it as just pretext—was Zuckerberg himself.

712. Just hours after sending his e-mail about Warren's call to breakup the company, Zuckerberg had an idea that would provide a privacy smokescreen while the company anticompetitively integrated its products to prevent divestiture:

Here's another way of thinking about this. If you asked any democratic presidential candidate whether Facebook should be able to integrate Instagram and WhatsApp, the politically popular answer would clearly be no. It wouldn't even be a tough decision. But if you asked whether we should have end-to-end encryption, that would put them in a much tougher position. I bet in the end they'd say yes with a bunch of dithering, but even if they came out at no, it would be much tougher for them. One of these issues is clearly more popular and sensitive than the other.

(PALM-006205414, at 15-16.)

713. In short, Zuckerberg realized that if he framed the back-end integration as about implementing end-to-end encryption (sometimes called "E2EE"), and therefore user privacy, instead of its actual purpose—preventing divestiture—the public, and perhaps even regulators, would be more likely to let Facebook go ahead with its plans.

714. The problem, of course, was that the back-end integration—the irreversible commingling of user data and processing architecture (among other things) from previously separate WhatsApp, Instagram, Facebook, and Messenger products—was totally distinct from end-to-end encryption. End-to-end encryption was (and is) the process of using hardware and/or software to convert certain communications into unreadable data (encryption) at a sending user's device, then using hardware and/or software to make that data readable again at a receiving user's device (decrypting)—and not decrypting that data at any point in between. This was a solved problem, even at Facebook: as the New York Times reported on April 5, 2016, citing WhatsApp's own company blog—

SAN FRANCISCO – WhatsApp, the messaging app owned by Facebook and used by more than one billion people, on Tuesday introduced full

FILED UNDER SEAL

1 encryption for its service, a way to ensure that only the sender and recipient
2 can read messages sent using the app.

3 Known as “end-to-end encryption,” it will be applied to photos, videos, and
4 group text messages sent among people in more than 50 languages across
5 the world”

6 715. In short, Facebook had long already possessed the technology, the know-how, the
7 resources, and indeed the business experience to introduce end-to-end encryption in any of its other
8 messaging services, and to its photo, video, and group text functions across its various products. Indeed,
9 ***Facebook had already done so in 2016, with WhatsApp.***

10 716. Moreover, encryption was, simply, a completely separate technical issue from integration.
11 Encrypting communications would not “integrate” anything (indeed, Facebook had chosen to end-to-end
12 encrypt WhatsApp, and nothing else, in 2016); and integrating multiple products would not suddenly
13 encrypt anything. The two technical concepts were—indisputably—totally distinct, and Zuckerberg knew
14 it.

15 717. However, using the phrase “end-to-end encryption” in any context did always bring one
16 predictable result: it immediately distracted from and overwhelmed any other technical issue in the
17 conversation, as law enforcement and civil libertarians would immediately fill the room with competing
18 views of electronic privacy at the mere mention of E2EE. The April 2016 New York Times article
19 announcing WhatsApp’s new end-to-end encryption was a case in point:

20 The move thrusts WhatsApp further into a standoff between tech
21 companies and law enforcement officials over access to digital data, one
22 that pits Silicon Valley’s civil libertarian ideals against the federal
23 government’s concerns over national security. Increased encryption will
24 make it more difficult, if not impossible, for the authorities to intercept
25 WhatsApp communications for investigations. . . .

26 End-to-end encryption for WhatsApp is of particular concern to the F.B.I.,
27 considering the service’s huge subscriber base and large international
28 footprint. With increasing amounts of communications now sent across
messaging services, encrypted texts, video, photos and the like may end up
being more problematic for law enforcement than locked devices. The
encryption on WhatsApp will be turned on by default, so users will not be
required to enable it themselves.

FILED UNDER SEAL

1 718. So when Facebook’s back-end integration—a completely distinct technical concept that
 2 would irreversibly commingle the data and architecture of four different Facebook products to prevent
 3 divestiture—was about to be thrust into the spotlight by Elizabeth Warren in March 2019, Zuckerberg
 4 quickly realized what smokescreen would best mask the truth: E2EE.

5 719. Nick Clegg responded favorably to Zuckerberg’s idea:

6 Are you suggesting we should lead with E2EE and not interoperability?
 7 You may be right that—as a matter of political practicality—the latter is
 8 easier to block/hinder than the former.

9 Where E2EE has a huge advantage over interoperability in the political
 10 debate is that it is very easy to explain why it is helpful to users—it protects
 11 their privacy—whereas integrating our messaging apps looks as much (if
 12 not more so, at least to our critics) as a play for our benefit, not necessarily
 13 users.

14 That is why handling the safety issues re: E2EE are so crucial—if we’re
 15 seen to be cavalier or careless, the first principle privacy argument will be
 16 swamped by controversy around the effect on public, partic child, safety.

17 (PALM-006205415.)

18 720. Meanwhile, as Zuckerberg directed his senior lieutenants to disseminate the newly-
 19 concocted privacy / encryption pretext for integration, he simultaneously pushed the end-to-end
 20 encryption narrative in the news and on his blog.

21 721. And virtually every news outlet reported near-exclusively on the propriety and
 22 background of end-to-end encryption and what it would mean for Facebook’s products.

23 722. Congress and the U.S. Department of Justice also focused almost exclusively on
 24 Facebook’s announcements about end-to-end encryption. As Engadget reported on October 3, 2019:

25 The Department of Justice is set to ask Facebook to pause plans for end-
 26 to-end encryption across all of its messaging services. It will urge the
 27 company not to move forward “without ensuring that there is no reduction
 28 to user safety.”

 Attorney General William Barr is set to make the request in an open letter
 to Facebook CEO Mark Zuckerberg on Friday. Acting Homeland Security
 Secretary Kevin McAleenan, UK Home Secretary Priti Patel and
 Australian Minister for Home Affairs Peter Dutton also signed the draft
 letter . . .

FILED UNDER SEAL

1 723. Facebook had successfully shifted the public and regulatory narrative away from
2 competitive concerns—and indeed, away from the actual details of the back-end product integration itself.
3 Attorney General William Barr and other regulators were almost entirely focused on serious problems
4 raised by Zuckerberg’s announced end-to-end encryption plans—namely, the risk that encryption could
5 hamper law enforcement efforts or facilitate child exploitation.

6 724. Internally, Facebook was executing on a plan far broader than end-to-end encryption—
7 one directed solely at making WhatsApp, Instagram, Facebook, and Messenger data, ML, and AI systems
8 indistinguishable—and inseverable—from each other before any regulator could act.

9 **F. Facebook Anticompetitively Integrates Its Products’ Back Ends, Creating Unified**
10 **Data Stores and AI/ML Systems**

11 725. Facebook’s integration plans internally were quite different than what Zuckerberg and
12 others at the company had publicly represented. In addition to building an end-to-end encryption
13 smokescreen, Facebook was frantically working to integrate AI and ML systems, as well as “features”
14 extracted from signals and social data.

15 726. The reason to integrate these systems was not to enhance Facebook’s technology. In fact,
16 the integration efforts made Facebook’s products less effective, less transparent, more expensive, less
17 flexible, and more difficult to debut and maintain. And, there was nothing wrong with the systems that
18 had existed prior to the integration; in many ways, those systems were superior.

19 727. The real reason for the integration was to inextricably intertwine the AI and ML systems
20 used across Facebook’s products, as well as the highly refined social data—the signals—used as inputs
21 to those systems. Facebook accomplished this in two primary ways: first, forcing the organization to build
22 AI and ML models from “features” rather than signals and raw social data; and second, pigeonholing
23 engineers and data scientists into a handful of AI and ML model architectures to be used across the
24 organization. Both of these things not only required Facebook and its affiliated businesses to abandon
25 technology that was bespoke to each product—technology that was immensely profitable and well
26 functioning—but also reduced the flexibility and efficacy of the AI and ML models powering Facebook’s
27 products. The sole and real (and the only rational or plausible technological) reason was to intertwine
28

FILED UNDER SEAL

1 data sources and AI/ML models across Facebook’s businesses, making them impossible to disaggregate
2 or operate independently. This was the ultimate defense to the looming threat of an antitrust breakup or
3 invasive regulatory oversight.

4 **1. Facebook Forces Its Products to Use Features Instead of Signals and Raw**
5 **Social Data to Build AI and ML Models, Making the Company’s Social Data**
6 **Impossible Disaggregate by Source or Line of Business.**

7 728. As part of Facebook’s integration push, the company created a massive aggregation of
8 “features,” with plans to require the entire organization to draw from the common features extracted from
9 features from different applications.

10 729. Facebook had already centralized “intent” data extracted from social data and signals, with
11 a central gatekeeping system to ensure that only appropriate systems could use particular social data and
12 signals that Facebook had extracted from social data.

13 730. This system was called the “Intent Platform,” and Facebook required authorization for
14 various groups at Facebook to use the “intent” data that was part of the platform. Importantly, the data
15 stored in the Intent Platform was rawer than what was ultimately extracted and used by Facebook’s AI
16 and ML systems.

17 731. If Facebook could force its businesses to use data that was the *composite* of less refined
18 social data, then it would obfuscate the ingredients of that composite and the source of the underlying
19 data. That is precisely what a focus on “features” rather than signals and social data would mean.
20 Facebook planned to force its organization to share features, meaning the raw signals and underlying
21 social data would be pre-processed and combined into features ready for processing by AI and ML models
22 across the organization.

23 732. Forcing data scientists and engineers across the organization had a massive downside: it
24 reduced their flexibility. An important part of developing an AI or ML model is selecting the features
25 that matter to inferences and predictions. That process requires significant trial and error—most
26 importantly, with varied sources of data. Ultimately, a particular model will be most effective with a
27 given set of “features”—which are extracted patterns in the underlying data. That process, including the
28

FILED UNDER SEAL

process of validating AI and ML models, often requires access to directly collected data, such as unprocessed social data from user Instagram feeds.

733. Features could be combined pieces of information from across Facebook’s apps. Once combined or refined into “features,” which Facebook internally described as a “superset” of “signals” collected from its apps, disaggregating the data to determine source would be in many cases impossible.

734. By February 2019, Facebook’s plan had been given a name: the “Facebook Feature Framework” or “F3.”

735. Although Facebook had maintained a database of “intent” information, which it internally referred to as the “Intent Platform,” Facebook planned to migrate to F3 across the organization. This would allow WhatsApp, Instagram, Facebook, Messenger, and other Facebook apps to consume features for machine learning from a unified, integrated source.

736. Jon Eide described the transition in a February 19, 2019, e-mail:

Data consumption through single interface: As discussed in data use principles proposal, we request all organic products to consume offsite data through single data source. Currently that is Signals Intent platform, later in 2019 will likely migrate it to F3—new Facebook Feature Framework, being implemented by Ads Infra, AI infra and Signals team and is meant to be company-wide platform for ML/intent data consumption. F3 will also have transparent privacy controls built in to manage which data is used for which scenarios.

(PALM-010434436.)

737. This migration would be incredibly disruptive to Facebook’s existing business. As such, Facebook engineers had to incrementally build the new F3 system and in many cases generate work that would be entirely wasted as a result.

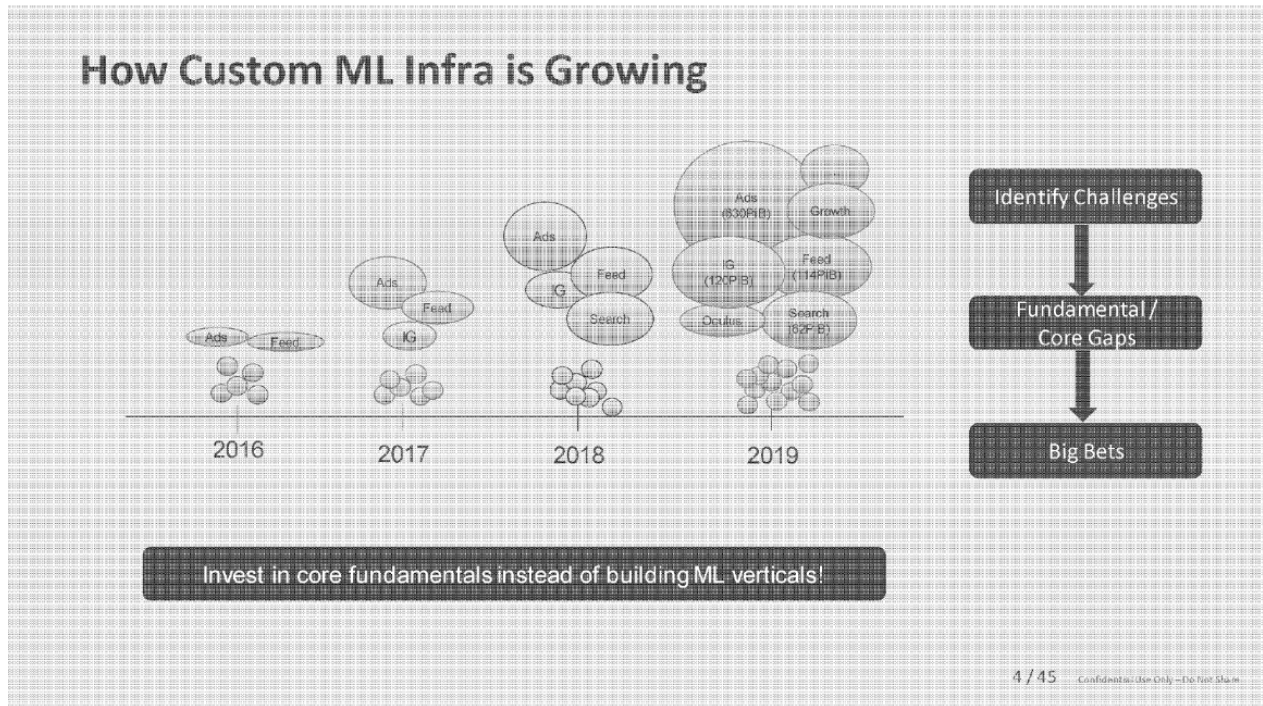
738. Moreover, Facebook’s existing systems needed continued access to rawer social data sources, particularly through Facebook’s massive database called “Hive” and Facebook’s existing “Intent Platform.”

739. As Facebook was removing AI and ML training flexibility from its various divisions, internal demand for custom AI and ML systems was growing significantly. As a Facebook “XFN” (or

FILED UNDER SEAL

Cross-Facebook) March 14, 2019, presentation showed, custom AI and ML demand, particularly for Instagram and Facebook's Ad targeting systems had exploded:
(PALM-010619603, at 07.)

740. At the same time, "feature engineering"—the process of determining what patterns in



underlying signals and social data were meaningful for AI and ML models—was “a major driver of revenue,” accounting for “45~55% of ads score contribution” in the first half of 2018. (*Id.* at 24.)

741. Facebook's push to centralize feature engineering directly clashed with the massive growth in demand for custom AI and ML models. Facebook's back-end integration would require Facebook's AI and Data infrastructure teams to become bottlenecks for the creation of new models.

742. Put simply, the centralization of “features” made no sense other than massively intertwining and obfuscating data sources across Facebook's products. Of course, the purpose of doing it was just that—irreversible commingling to avoid divestiture or invasive regulation. If Facebook succeeded in its feature integration efforts, it would become virtually impossible to break the company up or meaningfully regulate it.

FILED UNDER SEAL**2. Facebook Centralizes AI and ML Model Architectures and Testing**

743. As part of its integration plans, Facebook also forced its organization to centralize the creation and testing of new AI and ML models. Facebook began the creation of a new system called “Mastercook,” which required Facebook’s AI infrastructure teams to pre-train ML and AI components for use across the company.

744. Mastercook required the completion of significant F3 milestones before it could be completed and tested. Facebook again created a massive internal bottleneck as the internal demand for custom AI had increased. Rather than allow Facebook’s businesses to build custom AI as needed, Facebook stalled them out, opting to instead create pre-trained systems and AI and ML architectures that would not necessarily fit uses across the entire organization.

745. Moreover, Mastercook forced Facebook to rely on a concept called “transfer learning,” where a model trained for one application can be adapted to another without the need for retraining. In other words, rather than allow Facebook’s products to build their own bespoke models suited to particular applications and datasets, Facebook impaired and impeded their ability to do so.

746. Again, the centralization of AI and ML model creation and testing in the Mastercook system did not make sense technically. In fact, Mastercook cost significantly more than the *status quo*, resulted in weaker and less predictive AI models, and made the AI models actually used more opaque to each division.

747. Critically, once an AI or ML model has been trained, it is almost impossible to determine what the model found significant to its predictions in the underlying data provided to it. This is called the “black box” problem, and Facebook’s migration to a centralized AI and ML creation and testing system exacerbated it. Now, Instagram engineers would, for example, be relying on models potentially pretrained on data they had never seen—and once those models were trained and adapted, it would be impossible to tell what data mattered most to predictions or where the underlying data came from. All of this was technically worse, not better, for Facebook.

748. However, combining this AI and ML centralization with the F3 initiative meant that the underlying data, signals, and AI / ML at Facebook would be inextricably intertwined. Although there was

FILED UNDER SEAL

1 no legitimate technical advantage to F3 and Mastercook—and indeed, obvious technical *disadvantages*
2 to Facebook’s engineers and data scientists—from both, requiring F3 and Mastercook across the entire
3 Facebook organization meant that divestiture would not be as simple as splitting up legacy companies
4 and products. Rather, Facebook’s entire AI and Feature Engineering infrastructure would break if
5 separated—that is, if separation was even possible after such integration.

6 749. Facebook’s Mastercook initiative, particularly in the face of explosive demand for custom
7 AI, made no technological sense. This was especially so if implemented alongside F3. Instead,
8 Facebook’s real reason for pushing the AI and ML centralization initiative alongside F3 as part of its
9 product integration was to prevent divestiture and regulation.

10 **G. Zuckerberg’s End-to-End Encryption Smokescreen Was Pretextual and Lacked a**
11 **Legitimate Technical Justification**

12 750. As part of its integration efforts, Facebook sought to combine the underlying data stores
13 for its messaging applications, including WhatsApp, Instagram, and Facebook’s Messenger. The
14 underlying user messages were to be mined for user “intent” information, then fed—in “feature” form—
15 to F3. Again, the purpose was to obfuscate the source of the data, particularly from invasive mining of
16 user conversations.

17 751. Facebook needed to mask this invasive aspect of its integration, so it relied on its
18 battletested playbook—pretending there was a privacy-based reason for the change. As Zuckerberg
19 recognized in his conversations with Nick Clegg and others, it was difficult to explain how creating a
20 massive store of intent-rich user data from private conversations was pro-competitive, particularly in light
21 of Facebook’s Cambridge Analytica scandal and the public calls to break up the company.

22 752. Facebook and Zuckerberg had to add something ostensibly privacy-related to the
23 integration so that it could sell the move to the public. To do that, Facebook ordered its engineers to
24 implement end-to-end encryption across certain parts of Facebook’s business as part of its integrated
25 messaging-based data mining system.

26 753. Of course, the integration and the end-to-end encryption had nothing in particular to do
27 with one other. Facebook could easily integrate its messaging systems and harvest data from them for its
28

FILED UNDER SEAL

1 F3 and Mastercook systems without implementing any form of encryption. In fact, the addition of end-
2 to-end encryption alongside F3 and Mastercook *more* difficult. It made Facebook's existing systems less
3 efficient, and it increased both engineering and real-time computation costs.

4 754. And, likewise, end-to-end encryption could have been implemented at the application
5 level without integrating the back-ends of the messaging systems or the feature extraction from the
6 messaging apps.

7 755. In fact, WhatsApp already had end-to-end encryption features as part of its messaging
8 Platform. As the WhatsApp website stated in April 2016:

9 Security by Default

10 WhatsApp's end-to-end encryption is available when you and the people
11 you message use the latest versions of our app. Many messaging apps only
12 encrypt messages between you and them, but WhatsApp's end-to-end
13 encryption ensures only you and the person you're communicating with
14 can read what is sent, and nobody in between, not even WhatsApp. This is
15 because your messages are secured with a lock, and only the recipient and
16 you have the special key needed to unlock and read them. For added
17 protection, every message you send has its own unique lock and key. All
18 of this happens automatically: no need to turn on settings or set up special
19 secret chats to secure your messages.

20 756. Again, WhatsApp posted about this on its company blog. The New York Times wrote an
21 article about it. Facebook knew how to implement end-to-end encryption within its products—and it had
22 already done it, years prior.

23 757. Indeed, WhatsApp had implemented end-to-end encryption in 2016, and nothing about
24 that feature required any form of integration with Instagram or Facebook Messenger. The purported
25 addition of “end-to-end encryption” in 2019 was not, as Facebook suggested, part and parcel with the
26 back-end integration. To the contrary, it had nothing to do with it.

27 758. Moreover, the implementation of back-end integration alongside Facebook's feature and
28 AI/ML obfuscation measures like F3 and Mastercook only further impaired Facebook's existing systems
and made integration efforts more technologically challenging, particularly because end-to-end

FILED UNDER SEAL

1 encryption could have easily been implemented on each app separately without injecting additional
2 complexity in the integration process.

3 759. In reality, the end-to-end encryption had been tacked onto Facebook's back-end
4 integration to disguise the true reasons for Facebook's scramble to intertwine its applications, their
5 underlying data, and Facebook's machine learning model.

6 760. However, the end-to-end encryption discussion paired with reports of Facebook's back-
7 end integration was nothing more than a pretext, devised by Mark Zuckerberg and his public relations
8 team to mask Facebook's anticompetitive scramble to prevent divestiture and regulation.

9 761. There was no legitimate technical (or non-anticompetitive) justification for the integration,
10 the simultaneous cross-app addition of end-to-end encryption, Facebook's transition to centralized
11 "feature" systems, and Facebook's insistence on pre-trained and pre-designed AI and ML systems and
12 models.

13 762. At the same time, these Facebook product changes that occurred in early 2019 and
14 continue (as far as Plaintiffs can discern based on limited discovery) to this day unquestionably
15 strengthened and fortified the DTBE and helped to maintain Facebook's dominance in the Social
16 Advertising Market, irreversibly bringing together massive quantities of social data for mining and
17 targeting by Facebook.

18 763. Facebook's integration-related product changes had an anticompetitive effect in the Social
19 Advertising Market because, among other things, these product changes indivisibly commingled data and
20 models from the previously distinct WhatsApp, Instagram, Facebook, and Messenger products in a way
21 that fortified the DTBE and further sealed off meaningful competition in the Social Advertising Market,
22 both (i) by creating the largest aggregation of social targeting data the world has ever known, and (ii) by
23 preventing or substantially limiting the divestiture or separation (including court-ordered divestiture
24 pursuant to regulatory decree—and the Federal Trade Commission is currently seeking just this) of
25 discrete social data from WhatsApp, Instagram, and Facebook / Messenger.

26 764. But the above was an intended feature, not a bug. As explained in the previous sections,
27 these anticompetitive product changes by Facebook beginning in 2019 were expressly intended to
28

FILED UNDER SEAL

commingle previously distinct data and models in such a way that Facebook could not be divested or meaningfully disaggregated by a court or regulator, thereby sealing off potential competition and maintaining Facebook's Social Advertising Monopoly. Moreover, as explained in the previous sections, these anticompetitive product changes lacked a legitimate technical (or non-anticompetitive) justification.

XII. THE RELEVANT MARKET

765. Plaintiffs are consumers and purchasers in the relevant market at issue in this case—the Social Advertising Market. Plaintiffs are direct purchasers of advertising products from Facebook and were anticompetitively harmed as participants in the Social Advertising Market.

A. The Social Advertising Market

766. The Social Advertising Market is a submarket of online advertising, the latter of which includes banner ads, search-based ads, and advertising on social networks. Social advertising, however, is not fungible or interchangeable with these other forms of online advertising. Indeed, social advertising allows advertisers to granularly target groups of users for ads by their attributes, including by the attributes of their networks.

767. Thus, because of the extensive ability to target advertisements to users on social media sites like Facebook, search and banner advertising are not reasonable substitutes.

768. Several relevant factors indicate that the Social Advertising Market is a distinct submarket of online advertising and more general advertising markets:

769. *Industry or public recognition of the submarket as a separate economic entity.* Social advertising is broadly considered to be distinct from other forms of advertising by market and industry participants. For example, the advertising company Outbrain describes the differences between social ads on its blog as follows:

Paid social ads are served via algorithms that define what the user might be interested in, based on past activity in their social accounts, such as likes, shares, and comments. Unlike search, which is a focused, goal-oriented activity, browsing on social is more relaxed. Think cat memes, vacation snaps, and fun quizzes. Nevertheless, the social platform has accumulated masses of data about every specific user, which can be leveraged to target specific audiences with ads that are likely to be of interest to them.

FILED UNDER SEAL

1 770. Outbrain explains that social ads are considered useful for a distinct purpose:

2 Social ads are best for targeting audience segments who may be interested
3 in your product or services, based on a range of targeting criteria—location,
4 age group, gender, hobbies, interests. Social networks, such as Facebook,
5 have advanced targeting capabilities, which means you can fine-tune your
6 targeting criteria to reach a very specific, high-quality audience.

7 771. Outbrain explains that search ads are different, as they “are great for targeting customers
8 when they are already looking for you (*i.e.*, they search your company name or product), or if they are
9 searching for a specific product, service, or piece of information that you can provide.” Outbrain also
10 distinguishes social advertising from other forms of online advertising, like discovery advertising.

11 772. Moreover, providers of business statistics such as statista.com also provide information as
12 to social media advertising as a distinct submarket of online and general advertising.

13 773. As another example, in March 2015, leading advertising publication AdAge referred to
14 Facebook’s Custom Audience targeting, which is unique to social advertising, as “potentially different
15 and more special because they have this richer level of data.”

16 774. Likewise, industry publication Marketing Land reported in an October 14, 2019 article
17 that media agency Zenith, which is owned by Publicis Media, predicted growth in the social media
18 advertising segment as distinguished from search and television advertising, with social media ads
19 coming in third behind television and paid search advertising.

20 775. On an October 23, 2012 earnings call, Facebook’s COO Sheryl Sandberg said, “On the
21 question of where advertisers are, as I’ve said before, we are a third [thing]. We’re not TV, we’re not
22 search. We are social advertising, and I would say our clients are on different parts of that adoption
23 curve.” Later, on a May 1, 2013 earnings call, Sandberg explained: “As I said before, the thing about
24 brand advertisers is that they got very used to TV, then they got very used to search, and we are a third
25 thing.”

26 776. Even academic articles, including those published in the Journal of Advertising, have
27 analyzed the market for social media advertising as a distinct segment, with well-defined engagement
28 characteristics.

FILED UNDER SEAL

1 777. *The product's peculiar characteristics and uses.* Social advertising has a distinct purpose
2 from other forms of advertising. Social advertising has different applications than other forms of online
3 advertising. Namely, social advertising allows granular targeting based on user attributes, user interests,
4 and group attributes. Moreover, because of the detailed amount of information that can be collected about
5 users as they engage on social media platforms, social advertising can seek out other users with similar
6 behavioral characteristics.

7 778. Facebook, for example, describes its own targeting capabilities as follows:

8 Facebook ads can be targeted to people by location, age, gender, interests,
9 demographics, behavior and connections. You can also use more advanced
10 targeting tools like Lookalike Audiences, which lets you target people
11 similar to the people who already engage with your business, or you can
12 layer your targeting options to select a more specific audience.

13 779. Facebook allows advertisers to create Lookalike audiences. Thus, unlike search or other
14 forms of advertising where the ad is created and placed to reach a preexisting audience, Facebook is able
15 to algorithmically combine a subset of its users to fit an advertisement. This capability is unique to social
16 advertising.

17 780. As Facebook explains on its website:

18 When you create a Lookalike Audience, you choose a source audience (a
19 Custom Audience created with information pulled from your pixel, mobile
20 app, or fans of your page). We identify the common qualities of the people
21 in it (for example, demographic information or interests). Then we deliver
22 your ad to an audience of people who are similar to (or “look like”) them.

23 781. Because of the level of granular data Facebook collects from its users, it can provide
24 targeting flexibility like no other advertising medium. As Facebook explains:

25 You can choose the size of a Lookalike Audience during the creation
26 process. Smaller audiences more closely match your source audience.
27 Creating a larger audience increases your potential reach, but reduces the
28 level of similarity between the Lookalike Audience and source audience.
We generally recommend a source audience with between 1,000 to 50,000
people. Source quality matters too. For example, if a source audience is
made up of your best customers rather than all your customers, that could
lead to better results.

FILED UNDER SEAL

782. Social advertising is also marked by the ability to algorithmically refine advertising targeting as users interact with the ads. For example, Facebook allows users to place a pixel on their website that is pulled off Facebook's servers when the site is accessed. Facebook is thus able to determine the efficacy of ads run on Facebook once the user transitions to an advertiser's own website. Over time, Facebook's advertising becomes more targeted and more effective in terms of particular advertising goals, such as lead generation or online purchases.

783. Other social networks, such as Twitter, provide similar targeting abilities. Twitter, for example, allows targeting based on location, language, device, age, and gender, but also allows for the targeting of audience types, including algorithmically tailored and custom-created audiences.

784. These targeting features, which are available on social advertising platforms, are not comparably available as part of other forms of online advertising, such as display and banner ads or search ads.

785. ***Unique production facilities.*** Social advertising requires data collected from users on an inherently social application. A user's search history, for example, will not provide enough data to create highly targeted advertising features, such as Facebook's Lookalike Audiences. Likewise, passive advertising, such as banner ads, or even general magazine or publication ads, provides little granular data that can then be used to further refine the targeting of advertising.

786. Providers of social advertising require specialized means of production because they must rely on data harvested from engagement among networks of users to facilitate highly targeted advertising. Platforms capable of delivering social advertising must therefore provide functionality such as image and video sharing, messaging, matchmaking, content sharing, and other inherently social features in order to obtain the data needed to allow for granular user and user network targeting.

787. Because social advertising allows iterative refinement of target audiences, a provider of social advertising must employ machine-learning or artificial intelligence algorithms that are trained on data collected from users as they interact and engage with content and advertising. As Facebook's head of its Applied Machine Learning Group, Joaquin Quiñonero Candela, told *Wired* magazine (emphasis in original):

FILED UNDER SEAL

1 **Facebook today cannot exist without AI.** Every time you use Facebook or
2 Instagram or Messenger, you may not realize it, but your experiences are
3 being powered by AI.

(emphasis added).

4 788. Other forms of advertising generally do not require sophisticated machine learning or
5 artificial intelligence. For years prior to the advent of modern machine learning techniques, search
6 engines such as Yahoo and Google used far less sophisticated algorithms to match user searches with
7 suggested websites and, in turn, advertisements. Traditional advertising, such as magazine or television
8 ads, require no algorithms at all, let alone artificial intelligence.

9 789. **Distinct customers.** Social advertising customers are distinct from search advertisers and
10 passive display advertisers. Moreover, social advertising is generally more effective at targeted
11 advertising rather than reaching a massive number of people.

12 790. Customers advertising on search engines are generally seeking priority among the search
13 results returned given a particular keyword. Customers advertising on social media platforms are
14 searching for users that fit a particular, predefined profile or set of characteristics. Small businesses that
15 do not generally have the budget to bid on coveted search results are nonetheless able to bid on granularly
16 defined audiences on a social media platform like Facebook.

17 791. **Distinct prices and sensitivity to price changes.** Social advertising prices are distinct from
18 other forms of advertising. In search-based advertising, certain search keywords are bid up by many
19 advertisers seeking to have their ads displayed as part of search results. This means that prices in certain
20 categories, such as legal or home improvement, will be significantly higher on search-based platforms
21 than on social advertising platforms like Facebook. For example, legal ads are on average \$1.32 on a
22 cost-per-click basis on Facebook, whereas they are \$6.75 on a cost-per-click basis on the Google Ads
23 platform. Likewise, consumer services ads are on average \$3.08 on a cost-per-click basis on Facebook's
24 platform vs. \$6.40 on Google Ads.

25 792. Because bidding on Google Ads and other search-based advertising is zero sum, meaning
26 only a certain number of ads can be coupled with a particular set of search keywords, pricing is more
27 sensitive to changes in demand.

FILED UNDER SEAL

1 793. Social advertising, however, allows granular targeting, avoiding much of the zero-sum
2 nature of other forms of advertising bidding. Moreover, social advertisers like Facebook can tailor
3 audiences, reducing the likelihood that advertisers will have to compete for the same display opportunity
4 at any given point in time.

5 794. Other general forms of advertising such as television and print are even more zero-sum,
6 as there are limited time slots or available pages in a newspaper or magazine. Pricing is thus more
7 sensitive to demand in these forms of advertising.

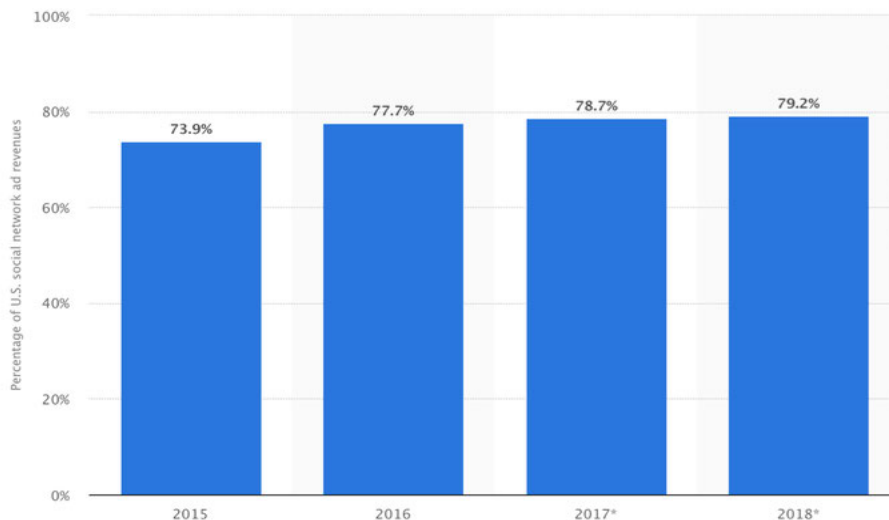
8 795. Social advertising is thus entirely distinct. Because of the ability to target audiences to
9 advertising, pricing is proportional to the generality of the targeting, not simply to the general demand
10 for a limited search term, key word, or periodical placement.

11 796. Moreover, Facebook has been able to consistently raise its prices in almost every year it
12 has sold advertising without facing price pressures from competitors. On a cost per mille (CPM)—or cost
13 per thousand advertising impressions—basis, Facebook’s advertising prices grew 90 percent year over
14 year according to a report at the end of 2019. In 2018, Vox reported that CPM prices on Facebook had
15 increased 122 percent year over year. In 2017, Facebook’s CPMs increased 171%. Facebook raised prices
16 in prior years as well.

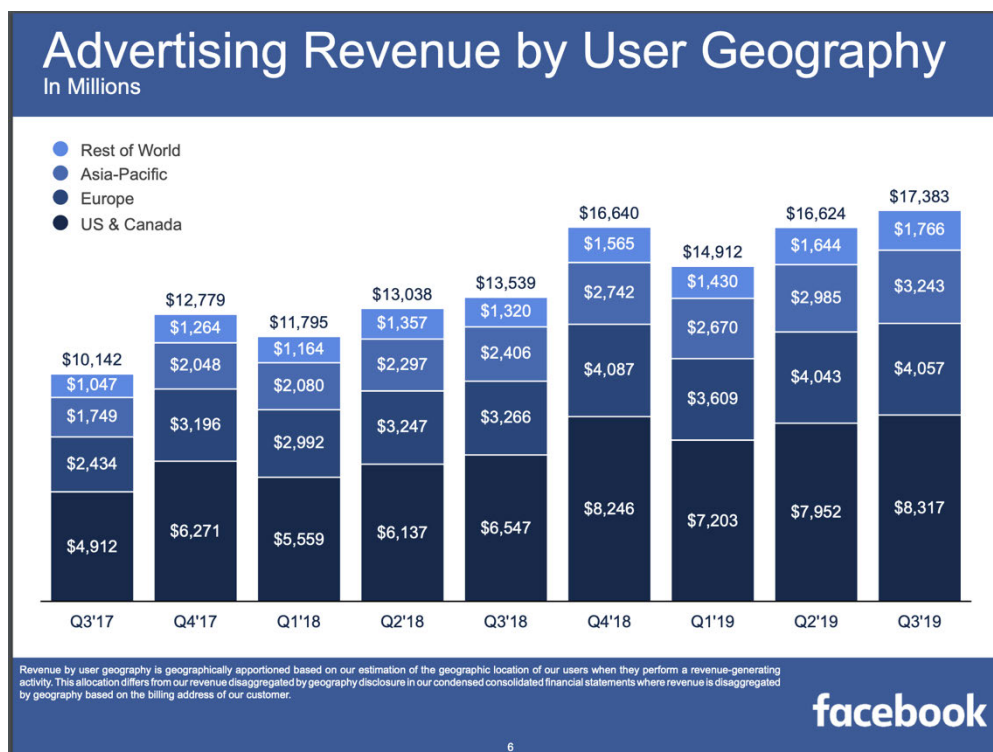
17 797. ***Specialized vendors.*** The Social Advertising Market has its own distinct and specialized
18 vendors, namely advertising agencies such as Lyfe, Thrive, Volume Nine, Sociallyin, and Firebelly
19 Marketing, all of which boast a specialization in social media advertising and provide specialized social
20 media management products. There are many such specialty advertising agencies that specialize in
21 creating social media advertising campaigns. Moreover, specialized social media analytics vendors also
22 exist, such as Socialbakers, which provides aggregated analytics across social media platforms. There is
23 an entire ecosystem of vendors specializing in social advertising—an indicator that the Social Advertising
24 Market is its own distinct submarket of online advertising, requiring its own unique tools and expertise.

FILED UNDER SEAL

798. Facebook's revenue share of the Social Advertising Market is approximately 80%. Its share has been above 70% since 2015. It remains above that threshold to this day.



799. Facebook's advertising revenue has steadily grown both in the United States and globally. Facebook reported advertising revenues totaling \$17.383 billion as of Q3 2019. Approximately \$8.3 billion of that advertising revenue came from the United States.



FILED UNDER SEAL

1 800. From 2014 to 2016, Facebook's advertising revenues grew from \$2.9 billion to \$6.436
2 billion. During that period, and even before then, Facebook was one of the few social networks that
3 significantly monetized its network by selling advertising. Other competitors did not come close, and
4 Facebook established unrivaled dominance in the Social Advertising Market and maintains that
5 dominance to this day.

6 801. Twitter, one of Facebook's only competitors to sell significant social advertising during
7 the same period Facebook generated revenue in the Social Advertising Market, has never exceeded \$800
8 million in advertising revenues. Revenues in Q1 2012 were approximately \$45 million, growing to \$432
9 million in Q4 2014, and standing at \$702 million as of Q3 2019.

10 802. LinkedIn, another competitor that sells social advertising, generated roughly \$2 billion in
11 overall annual revenue by the end of 2018, with some portion of that coming from advertising.

12 803. Considering the revenue generated by LinkedIn and Twitter, Facebook's advertising
13 revenue accounts for approximately 86% of the total revenue share across the three largest firms
14 competing in the Social Advertising Market. Excluding the contributions from minor competitors that
15 monetize their social networks, the HHI of the Social Advertising Market is approximately 7,685, well
16 beyond what the DOJ considers a highly concentrated market.

17 **B. Barriers to Entry**

18 804. The Social Advertising Market is protected by the Data Targeting Barrier to Entry that
19 prevents Facebook's competitors from entering the market. Without a critical mass of social data and
20 machine-learning / AI technology, market participants in the Social Advertising Market cannot generate
21 revenue.

22 805. Moreover, without adequate social data and engagement with the social network, market
23 participants cannot display content to users that would provide enough value to generate engagement and
24 additional social data.

25 806. Likewise, without a critical mass of social data, advertising targeting will not be possible
26 or will be substantially diminished in effectiveness, thus reducing revenues in the advertising sales in the
27 Social Advertising Market.
28

FILED UNDER SEAL

1 807. A firm's market power in this market therefore depends on obtaining a critical mass of
2 social data and the technology to mine it. Because of network effects, users will not use a social network
3 that lacks enough social data to provide targeted content or to provide valuable connections to other users.
4 However, once a certain amount of social data is obtained by a market participant, a feedback loop may
5 form as a result of network effects, further increasing the amount of social data generated by the social
6 network.

7 808. A new entrant must therefore expend significant amounts of investments in capital,
8 technology and labor to create a network large enough to create the network effects necessary to compete
9 with dominant firms in the market.

10 809. Because of the large amount of capital and social data required to successfully enter the
11 Social Advertising Market, the DTBE effectively excludes entry by a new competitor, even a well-funded
12 one. Indeed, the DTBE prevented Google from successfully entering the market for social data and the
13 Social Advertising Market with its Google+ social networking product.

14 810. Although Google+ had successfully replicated Facebook's core functionality and even
15 added additional functionality to its software, its entry failed because it lacked the critical mass of social
16 data that is required to reverse the network effects protecting Facebook. Without that critical mass, users
17 will not incur the costs of switching from Facebook's social network to a new entrant's social network.
18 That is, a new entrant will not be able to provide a valuable network of engaged users upon entry to justify
19 a Facebook user to change social networks.

20 811. That is precisely what happened to Google. Although it had a massive user base, it lacked
21 engagement, which meant it did not provide a sufficient amount of social data that could be used to target
22 content and advertising to users. This, in turn, reduced the value of the entrant social network and
23 accordingly the attraction of switching from Facebook's social network to Google's.

24 812. The DTBE continues to reinforce Facebook's dominant position. In fact, by excluding
25 rivals and potentially competing social networks through the anticompetitive scheme described in this
26 Complaint, Facebook strengthened the DTBE, providing it a larger share of social data and a stronger
27
28

FILED UNDER SEAL

monetization channel through social advertising. The additional amount of social data increases the value of its network, and the revenue from social advertising increases the cost of entry for a new rival.

813. Other barriers to entry in the Social Advertising Market include, but are not limited to, the high cost of development, data management, talent acquisition and retention, server infrastructure, development infrastructure, software technology, software libraries, and a brand and marketing presence sufficient enough to attract an engaged user base.

C. Relevant Geographic Market

814. The relevant geographic market is the United States Social Advertising Market.

815. For the social data that fuels a social advertising product, social data must be compatible with the customers purchasing that data. Thus, social data about a foreign market may be of little use for a U.S.-based advertiser. The data may be collected in a different language, may involve interests more pertinent to a particular geographic region (*e.g.*, American Football vs. Rugby), and may contain a demographic of users that share a common culture or merely a close proximity.

816. The same is true for the Social Advertising Market. An advertiser seeking to sell products designed for consumption in the United States may not have any use for a platform's advertising targeting capabilities outside of the United States. In the U.S., Facebook enjoys a higher market share of the Social Advertising Market than it does worldwide (which is already very high, as described in subsection VI.A). In short, Facebook enjoys an even more dominant share of the U.S. Social Advertising Market than it does globally.

817. In the U.S., Facebook's market share of the social data generated by users is even greater than its global market share. Services such as WeChat are geared towards Asian markets, particularly China, and do not generally compete in the U.S. market with Facebook's Messenger, Instagram, and core social networking product. Thus, Facebook's U.S.-based market share is even higher than its global market share referenced above in VI.A, which is already a dominant share of the Social Advertising Market.

FILED UNDER SEAL**XIII. HARM TO COMPETITION AND ANTITRUST INJURY**

818. Facebook's anticompetitive scheme had the purpose and effect of monopolizing the Social Advertising Market in the United States. Facebook's conduct allowed it to maintain the monopoly and market power it had obtained by 2010 in the Social Advertising Market, and/or Facebook intended and attempted to acquire such a monopoly through its anticompetitive scheme.

819. Specifically, Facebook engaged in a series of acts in furtherance of its scheme, including, but not limited to:

- the targeting of competitors for coercive Whitelist and Data Sharing Agreements on pain of denial of access to Facebook's Platform and APIs, including Facebook's Events APIs;
- entering into targeted "sub-verticals" including e-commerce (Marketplace), location-based services (Places API), and streaming video (Facebook Watch), to obtain signal for data targeting, then leveraging the threat of competition from these subvertical products to enter into anticompetitive agreements with eBay, Foursquare, and Netflix that collusively weakened Facebook's sub-vertical products while fortifying the DTBE around Facebook's Social Advertising monopoly, and further protecting that monopoly against actual or potential competition in the Social Advertising Market;
- using deceptively-obtained Onavo data to identify and surveil competitive threats, train AI / ML models using information not reasonably available to potential Social Advertising competitors and/or entrants, thereby maintaining the DTBE and Facebook's Social Advertising monopoly;
- entering into an anticompetitive agreement with Google to bolster and reinforce Facebook's dominant position in the Social Advertising Market; and
- anticompetitively integrating AI/ML Models and features from across distinct products and data sources in a manner that reinforced the DTBE and maintained Facebook's Social Advertising monopoly.

820. This conduct, each individually, and together as a whole, harmed competition in at least the following ways:

FILED UNDER SEAL

821. *First*, Facebook’s conduct resulted in the exclusion of actual and potential competitors from the Social Advertising Market. By entering into a series of anticompetitive whitelist and data sharing agreements after scuttling its Platform, Facebook was able to obtain a superset of the social data collected by third-party apps. Facebook leveraged deprecation decisions, including as to the Events APIs, to obtain social data and signals from third parties. Facebook also entered into anticompetitive deals with Netflix, eBay, and Foursquare that allowed Facebook to capture additional social data it could use as part of its advertising targeting without having to engage in fierce competition to get it. Facebook fended off the threat beyond its walled garden with an anticompetitive agreement with Google. Facebook used deception to obtain through Onavo spyware user information that ordinary competitors would not have access to—and used that information to surveil competitive threats and to train Facebook’s ML and AI models. And, Facebook scrambled to integrate AI and ML “features” and forced its organization to use pre-trained and pre-packaged AI/ML models in order to inextricably intertwine data and AI/ML from its WhatsApp, Instagram, Messenger, and Facebook businesses. This conduct collectively ensured that a rival Social Advertising Platform could not enter the market and that regulators could not break up Facebook or otherwise regulate its conduct.

822. *Second*, Facebook’s conduct reduced consumer choice / welfare. Facebook’s conduct ensured that there would be no competition by a rival social advertising platform on non-price bases, such as, for example, increased privacy, more features, higher quality features, new features, more valuable social connections, reduced advertising to users, or new use cases. The scheme also foreclosed new or alternate business models by competitors or potential competitors.

823. Additionally, Facebook’s Onavo surveillance system exfiltrated personal and sensitive data from user devices, then stored that data in Facebook’s massive database, the “Hive.” Facebook was able to take user data from users even if they were not using Facebook’s apps. Facebook deceived users about its Onavo Apps, including Onavo Protect. Facebook used all of the exfiltrated data to build Machine Learning and AI systems as well as other statistical models that provided it real-time insights into competition and user behavior. Users were not given a choice as to how their data was collected, the extent of data collected, and how their data was ultimately used by Facebook. Moreover, this stolen

FILED UNDER SEAL

1 Onavo data was not available to rivals or potential entrants in the Social Advertising Market, ensuring
2 that there would be no competitive price check to Facebook's supracompetitive social advertising prices.

3 824. Likewise, user data was incorporated into Facebook's advertising targeting systems by
4 virtue of anticompetitive agreements with Foursquare, Netflix, and eBay. The net result was to strengthen
5 Facebook's position in the Social Advertising Market, reducing the ability of other firms to enter the
6 market, particularly without access to the social data streams and signals Facebook obtained by
7 threatening competition with, and capturing data from, these companies.

8 825. Facebook also reduced advertising consumer choice. Because of Facebook's conduct,
9 Facebook's targeting ability vastly increased and the ability of a potential competitor to access a
10 meaningfully unique store of social data was sealed off, preventing other social advertising companies
11 from entering the Social Advertising Market. This resulted in fewer Social Advertising choices for
12 advertisers and left only Facebook's monopoly rents as available prices in the Social Advertising Market.

13 826. *Third*, Facebook's conduct allowed it to raise prices. Facebook's anticompetitive scheme
14 has allowed it to raise prices for social advertising during and the execution of the scheme and Facebook's
15 course of conduct, including across both class periods. Facebook continues to be one of the only sources
16 for targeted social advertising in the United States and in most of the world. As evidence of its market
17 power in the Social Advertising Market, Facebook has raised prices without sacrificing any demand.

18 827. For example, Facebook's requirement that developers purchase advertising as a condition
19 of maintaining access to Platform features artificially created demand for Facebook's advertising
20 products, particularly its mobile advertising product. This had the purpose and effect of directly inflating
21 advertising prices.

22 828. Similarly, Facebook's anticompetitive deals with eBay and Netflix—in which Facebook
23 pulled back on competition in those companies' principal markets in return for large, nine-figure ad
24 purchases—inflated demand for Facebook's Social Advertising products, with the purpose and effect of
25 inflating advertising prices in that market. Moreover, these same agreements—and Facebook's agreement
26 with Foursquare—provided Facebook with valuable signal data that bolstered and maintained the DTBE
27 around Facebook's social advertising business, prevented meaningful competition by a would-be
28

FILED UNDER SEAL

competitor armed with those companies' social data, and ultimately allowed Facebook to maintain and raise prices in the Social Advertising Market with little or no competitive check in the months and years following those agreements.

829. In addition, Facebook's anticompetitive agreement with Google allowed Facebook to track Facebook, Instagram, and WhatsApp users outside of those applications and gave Facebook priority when advertising to them. As a result of that agreement, Facebook did not meaningfully compete with Google in programmatic and display-based advertising product markets and sub-markets, and Google did not leverage its ability to identify and target Facebook users, which would diminish Facebook's dominance over targeted advertising to those users while on Facebook's social network. Because Google bolstered and reinforced Facebook's dominant position and market power in the Social Advertising Market, Facebook was able to maintain and raise prices with little or no competitive check.

830. Next, by strengthening the DTBE, eliminating competition and preventing competitive entry, and by capturing user social data from various sources through the conduct set forth in this Complaint, including by entering into a series of anticompetitive whitelist agreements with targeted developers after scuttling its Platform; entering into anticompetitive deals with Netflix, eBay, and Foursquare that allowed Facebook to capture additional social data for its advertising targeting; entering into an anticompetitive agreement with Google; using deception to obtain data competitors did not have access to, which data was used to surveil competitive threats and train Facebook's ML and AI models; and scrambling to integrate AI and ML "features" and forcing a backend integration to inextricably intertwine data and AI/ML from its WhatsApp, Instagram, Messenger, and Facebook businesses, Facebook was able to charge supracompetitive prices without any meaningful check.

831. *Fourth*, Facebook's conduct strengthened the DTBE, creating a protective moat around Facebook's monopoly. Facebook's conduct fortified and expanded Facebook's access to vital social data, including signals from what Facebook described as "sub-verticals." Facebook entered into a series of anticompetitive agreements that provided it with data and AI/ML that allowed it to prevent entry by rivals. Facebook's strengthening of the DTBE was calculated to ensure that any rival entering the Social Advertising market would have to obtain a critical mass of social data, AI / ML infrastructure, and real-

FILED UNDER SEAL

1 time surveillance capabilities in order to viably compete with Facebook upon entry, making such an entry
2 effectively cost-prohibitive.

3 832. Each of Facebook's exclusionary acts lack any procompetitive benefit / justification, let
4 alone any justification that could outweigh the anticompetitive effects of the acts. For example,
5 Facebook's agreements with Netflix, eBay, and Foursquare are anticompetitive agreements to cease
6 competing in the streaming video, e-commerce, and location sub-verticals, respectively, in exchange for
7 obtaining user data (and, for Netflix and eBay, substantial ad purchases) from each company.

8 833. The anticompetitive effects of these agreements, including the strengthening of
9 Facebook's DTBE, far outweigh any procompetitive effects of dividing markets with each company (and
10 the facts as alleged in this complaint demonstrate that there are none). There are likewise no
11 procompetitive effects that outweigh the anticompetitive effects of Facebook's extended API agreements
12 and other Platform conduct, including its Events API conduct. There is also no legitimate, non-pretextual
13 technical justification for Facebook's backend integration.

14 834. The net effect of Facebook's anticompetitive conduct was to inflate advertising prices,
15 including the prices paid by Plaintiffs and the Classes. In the alternative, Facebook's conduct described
16 in this complaint had the purpose and effect of achieving a dangerous probability of a monopoly in the
17 United States Social Advertising Market.

18 835. All of this has resulted in sustained and increasing supracompetitive prices for Facebook
19 advertisements. Each of the Plaintiffs (and the persons, entities, and companies in the proposed Classes)
20 bought Facebook advertisements at supracompetitive prices inflated by Facebook's anticompetitive
21 scheme.

22 836. Plaintiffs therefore were, and are, harmed in their business and property: they were
23 overcharged for advertising as a result of unlawful, anticompetitive conduct by Facebook.

CLASS ACTION ALLEGATIONS

24
25 837. The Classes' claims all derive directly from a course of conduct by Facebook. Facebook
26 has engaged in uniform and standardized conduct toward the class. Facebook did not materially
27 differentiate in its actions or inactions toward members of the class. The objective facts on these subjects
28

FILED UNDER SEAL

are the same for all class members. Within each Claim for Relief asserted by the class, the same legal standards govern. Accordingly, Plaintiffs bring this lawsuit as a class action on their own behalf and on behalf of all other persons similarly situated as members of the proposed class pursuant to Federal Rules of Civil Procedure 23(a) and (b)(3) and/or (b)(2) and/or (c)(4). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions.

The Pre-2018 Nationwide Advertiser Class

838. Between October 1, 2012, and April 3, 2018, Facebook advertisers, including Plaintiffs Affilious, Jessyca Frederick, Joshua Jeon, and 406 Property Services were governed by materially common terms of service, which applied generally to both commercial and non-commercial Facebook accounts during this period.

839. Plaintiffs Affilious, Jessyca Frederick, Joshua Jeon, and 406 Property Services bring this action and seek to certify and maintain it as a class action under Rules 23(a); (b)(2); and/or (b)(3); and/or (c)(4) of the Federal Rules of Civil Procedure on behalf of themselves and a Pre-2018 Nationwide Advertiser Class defined as follows:

All persons, entities, and/or corporations in the United States who purchased advertising from Facebook between December 1, 2016, and April 3, 2018, but not after April 3, 2018, and were thereby injured by anticompetitive price inflation in the Social Advertising Market (the “Pre-2018 Class Period”).

840. Excluded from the Pre-2018 Nationwide Advertiser Class is the Post-2018 Nationwide Advertiser Class, Facebook, its employees, officers, directors, legal representatives, heirs, successors, and wholly or partly owned subsidiaries or affiliates; and the judicial officers and their immediate family members and associated court staff assigned to this case.

The Post-2018 Nationwide Advertiser Class

841. Between April 4, 2018, and the present, Facebook advertisers, including Plaintiffs Mark Berney, Mark Young, and Katherine Looper, have been governed by materially common terms of service, which applied specifically to “commercial” Facebook accounts during this period.

FILED UNDER SEAL

1 842. Plaintiffs Mark Berney, Mark Young, and Katherine Looper, bring this action and seek to
2 certify and maintain it as a class action under Rules 23(a); (b)(2); and/or (b)(3); and/or (c)(4) of the
3 Federal Rules of Civil Procedure on behalf of themselves and a Post-2018 Nationwide Advertiser Class
4 defined as follows:

5 All persons, entities, and/or corporations in the United States who
6 purchased advertising from Facebook between April 4, 2018, and the
7 present, and were thereby injured by anticompetitive price inflation in the
8 Social Advertising Market (the “Post-2018 Class Period”).

8 843. Excluded from the Post-2018 Nationwide Advertiser Class is the Pre-2018 Nationwide
9 Advertiser Class, Facebook, its employees, officers, directors, legal representatives, heirs, successors,
10 and wholly or partly owned subsidiaries or affiliates; and the judicial officers and their immediate family
11 members and associated court staff assigned to this case.

Numerosity and Ascertainability

12
13 844. Each class in this action satisfies the requirements of Fed. R. Civ. P. 23(a)(1). Thousands
14 of persons, entities, and/or companies nationwide purchased advertising from Facebook in each of the
15 Pre-2018 and Post-2018 Class Periods. Individual joinder of all Class members is impracticable.

16 845. The Classes are ascertainable because their members can be readily identified using
17 Facebook accounts, Facebook Ads registrations, and other records and information kept by Facebook or
18 third parties in the usual course of business and within their control. Plaintiffs anticipate providing
19 appropriate notice to the certified Classes, in compliance with Fed. R. Civ. P. 23(c)(1)(2)(A) and/or (B),
20 to be approved by the Court after class certification, or pursuant to court order under Fed. R. Civ. P.
21 23(d).

Predominance of Common Issues

22
23 846. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) because
24 questions of law and fact that have common answers that are the same for each Class predominate over
25 questions affecting only individual Class members.

26 847. Common issues include, without limitation, the following questions of law and fact for
27 both the Pre-2018 and Post-2018 Nationwide Advertiser Classes:
28

FILED UNDER SEAL

- a. Whether Defendant monopolized the Social Advertising Market.
- b. Whether Defendant, its employees or affiliates, intended to monopolize the Social Advertising Market.
- c. Whether Defendant attempted to monopolize the Social Advertising Market.
- d. Whether Defendant possessed monopoly or market power in the Social Advertising Market.
- e. Whether user data and data obtained by third parties created a Data Targeting Barrier to Entry that protected Facebook's market position and/or monopoly, reduced competition or entry in the Social Advertising Market, and/or increased prices for products in that market, including, but not limited to, advertising sold to members of the proposed Classes.
- f. Whether Defendant's agreements with whitelisted developers violated Section 2 of the Sherman Act, including whether the agreements restrained trade or strengthened the Data Targeting Barrier to Entry.
- g. Whether Defendant's "entry and capture" conduct, as described and alleged in this complaint, violates Section 2 of the Sherman Act;
- h. Whether Defendant's "entry and capture" agreement with Netflix, as described and alleged in this complaint, violates Section 1 of the Sherman Act;
- i. Whether Defendant's "entry and capture" agreement with eBay, as described and alleged in this complaint, violates Section 1 of the Sherman Act;
- j. Whether Defendant's agreement with Google to reinforce and bolster Facebook's dominance in the Social Advertising Market violated Sections 1 and 2 of the Sherman Act.
- k. Whether Defendant's back-end integration is anticompetitive and violates Section 2 of the Sherman Act;
- l. Whether Defendant's conduct harmed competition in the Social Advertising Market.

FILED UNDER SEAL

m. Whether Defendant's conduct caused price increases or the reduction of consumer or developer choice in the Social Advertising Market.

n. Whether Defendant's unlawful conduct was a substantial contributing factor in the injury to members of the Classes.

Typicality

848. This action satisfies the requirements of Fed. R. Civ. P. 23(a)(3) because for each proposed Class, the identified Plaintiffs' claims are typical of the claims of other Class members and arise from the same course of conduct by Defendant. The relief that each Class's named Plaintiffs seek is typical of the relief sought for the absent Class members.

Adequate Representation

849. Plaintiffs will fairly and adequately represent and protect the interests of the Classes. Plaintiffs have retained counsel with substantial experience in prosecuting antitrust and consumer class actions.

850. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the Classes and have the financial resources to do so. Neither Plaintiffs nor their counsel have interests adverse to those of the Classes.

Superiority

851. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(2) because Defendant has acted and refused to act on grounds generally applicable to the Classes, thereby making appropriate final injunctive and/or corresponding declaratory relief with respect to the Classes as a whole.

852. This action satisfies the requirements of Fed. R. Civ. P. 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of this controversy. For each proposed Class, the common questions of law and fact regarding Defendant's conduct and responsibility predominate over any question affecting only individual Class members.

853. Because the damages suffered by each individual Class member may be relatively smaller than the costs of litigation, the expense and burden of individual litigation would make it very difficult or impossible for individual Class members to redress the wrongs done to each of them individually, such

FILED UNDER SEAL

1 that most or all Class members would have no rational economic interest in individually controlling the
2 prosecution of specific actions, and the burden imposed on the judicial system by individual litigation by
3 even a small fraction of the Class would be enormous, making class adjudication the superior alternative
4 under Fed. R. Civ. P. 23(b)(3)(A) for each of the proposed Classes.

5 854. For each of the proposed Classes, the conduct of this action as a class action presents far
6 fewer management difficulties, far better conserves judicial resources and the parties' resources, and far
7 more effectively protects the rights of each Class member than would piecemeal litigation. Compared to
8 the expense, burdens, inconsistencies, economic infeasibility, and inefficiencies of individualized
9 litigation, the challenges of managing this action as a class action are substantially outweighed by the
10 benefits to the legitimate interests of the parties, the court, and the public of class treatment in this Court,
11 making class adjudication superior to other alternatives, under Fed. R. Civ. P. 23(b)(3)(D).

12 855. Plaintiffs are not aware of any obstacles likely to be encountered in the management of
13 this action that would preclude its maintenance as a class action. Rule 23 provides the Court with authority
14 and flexibility to maximize the efficiencies and benefits of the class mechanism and reduce management
15 challenges. The Court may, on motion of Plaintiffs or on its own determination, certify nationwide,
16 statewide, and/or multistate classes for claims sharing common legal questions; utilize the provisions of
17 Rule 23(c)(4) to certify any particular claims, issues, or common questions of fact or law for class-wide
18 adjudication; certify and adjudicate bellwether class claims; and utilize Rule 23(c)(5) to divide any class
19 into subclasses.

REALLEGATION AND INCORPORATION BY REFERENCE

20
21 856. Plaintiffs reallege and incorporate by reference all the preceding paragraphs and
22 allegations of this Complaint, as though fully set forth in each of the following Claims for Relief asserted
23 on behalf of the Classes.

FILED UNDER SEAL

CLAIMS FOR RELIEF

COUNT I

**Section 2 Sherman Act:
Monopolization**

857. Defendant has willfully acquired and maintained monopoly power in the relevant market for Social Advertising.

858. Facebook possesses monopoly power in the relevant market for Social Advertising. Facebook has the power to control prices or exclude competition in the relevant market.

859. Facebook's revenue share of the Social Advertising Market is approximately 80%; its share has been above 70% since 2015.

860. Defendant has willfully acquired and maintained monopoly power for Facebook in the relevant market for Social Advertising. As alleged in this Complaint, Defendant has accomplished this by means of predatory, exclusionary, and anticompetitive conduct, including but not limited to:

- the targeting of competitors for coercive Whitelist and Data Sharing Agreements on pain of denial of access to Facebook's Platform and APIs, including Facebook's Events APIs;
- entering into targeted "sub-verticals" including e-commerce (Marketplace), location-based services (Places API), and streaming video (Facebook Watch), to obtain signal for data targeting, then leveraging the threat of competition from these subvertical products to enter into anticompetitive agreements with eBay, Foursquare, and Netflix that collusively weakened Facebook's sub-vertical products while fortifying the DTBE around Facebook's Social Advertising monopoly, and further protecting that monopoly against actual or potential competition in the Social Advertising Market;
- using deceptively-obtained Onavo data to identify and surveil competitive threats, and to train AI / ML models using information not reasonably available to potential Social Advertising competitors and/or entrants, thereby maintaining the DTBE and Facebook's Social Advertising monopoly;
- entering into an anticompetitive agreement with Google to bolster and reinforce Facebook's dominant position in the Social Advertising Market; and

FILED UNDER SEAL

- anticompetitively integrating AI/ML Models and features from across distinct products and data sources in a manner that reinforced the DTBE and maintained Facebook’s Social Advertising monopoly.

861. Defendant’s conduct alleged here has had an anticompetitive effect in the relevant market for Social Advertising.

862. Defendant’s conduct alleged here has no legitimate business purpose or procompetitive effect.

863. Defendant’s conduct alleged here has had a substantial effect on interstate commerce.

864. Plaintiffs and the Classes have been and will be injured in their business or property as a result of Defendant’s conduct alleged in this Complaint.

865. Plaintiffs and the Classes have suffered and will suffer injury of the type that the antitrust laws were intended to prevent by reason of Defendant’s conduct. Plaintiffs and the Classes have been and will be injured by the harm to competition as a result of Defendant’s conduct.

COUNT II
Section 2 Sherman Act:
Attempted Monopolization

866. As alleged in this Complaint, Defendant has engaged in predatory, exclusionary, and anticompetitive conduct, including but not limited to:

- the targeting of competitors for coercive Whitelist and Data Sharing Agreements on pain of denial of access to Facebook’s Platform and APIs, including Facebook’s Events APIs;
- entering into targeted “sub-verticals” including e-commerce (Marketplace), location-based services (Places API), and streaming video (Facebook Watch), to obtain signal for data targeting, then leveraging the threat of competition from these subvertical products to enter into anticompetitive agreements with eBay, Foursquare, and Netflix that collusively weakened Facebook’s sub-vertical products while fortifying the DTBE around Facebook’s Social Advertising monopoly, and further protecting that monopoly against actual or potential competition in the Social Advertising Market;

FILED UNDER SEAL

- using deceptively-obtained Onavo data to identify and surveil competitive threats, and to train AI / ML models using information not reasonably available to potential Social Advertising competitors and/or entrants, thereby maintaining the DTBE and Facebook's Social Advertising monopoly;
- entering into an anticompetitive agreement with Google to bolster and reinforce Facebook's dominant position in the Social Advertising Market; and
- anticompetitively integrating AI/ML Models and features from across distinct products and data sources in a manner that reinforced the DTBE and maintained Facebook's Social Advertising monopoly.

867. Defendant's conduct alleged here has had an anticompetitive effect in the relevant market for Social Advertising.

868. Defendant's conduct alleged here has no legitimate business purpose or procompetitive effect.

869. Defendant has engaged in this conduct with the specific intent of monopolizing the relevant market for Social Advertising.

870. Defendant has engaged in this conduct with a dangerous probability of monopolizing the relevant market for Social Advertising.

871. Defendant's conduct alleged here has had a substantial effect on interstate commerce.

872. Plaintiffs and the Classes have been and will be injured in their business or property as a result of Defendant's conduct alleged in this Complaint.

873. Plaintiffs and the Classes have suffered and will suffer injury of the type that the antitrust laws were intended to prevent by reason of Defendant's conduct. Plaintiffs and the Classes have been and will be injured by the harm to competition as a result of Defendant's conduct.

COUNT III
Section 1 Sherman Act:
Restraint of Trade

FILED UNDER SEAL

874. As alleged in this Complaint, Facebook knowingly and intentionally entered into an agreement to restrict trade in order to preserve the DTBE and protect Facebook's control of social advertising. This agreement, by bolstering and reinforcing Facebook's market power and dominance in the Social Advertising Market, had the purpose and effect of maintaining market divisions and/or segmentation, allowing Facebook to continue charging a significant price premium for its targeted advertising sold in the Social Advertising Market. Because of this agreement, no fungible level of targeted advertising would emerge that could rival Facebook's ad products.

875. Defendant's conduct alleged above is a *per se* violation of Section 1 of the Sherman Act, 15 U.S.C. § 1. Plaintiffs therefore do not need to allege a relevant market. To the extent a market must be alleged, Facebook's restraint of trade has had an anticompetitive effect in the relevant market of Social Advertising in the United States.

876. Defendant's conduct alleged here has no legitimate business purpose or procompetitive effect.

877. Defendant's conduct has had a substantial effect on interstate commerce.

878. Plaintiffs and the Classes have been and will be injured in their business or property as a result of Defendant's conduct alleged here.

879. Plaintiffs and the Classes have suffered and will suffer injury of the type that the antitrust laws were intended to prevent by reason of Defendant's conduct. Plaintiffs and the Classes have been and will be injured by the harm to competition as a result of Defendant's conduct.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request that judgment be entered against Defendant and that the Court grant the following:

- A. Determine that this action may be maintained as a class action pursuant to Rules 23(a), (b)(2), (b)(3) and/or (c)(4) of the Federal Rules of Civil Procedure, and direct that reasonable notice of this action, as provided by Rule 23(c)(2), be given to the Classes, and declare Plaintiffs as the representatives of the Classes;
- B. Enter a judgment against Defendant in favor of Plaintiffs and the Classes;

FILED UNDER SEAL

- 1 C. Award the Classes damages (i.e., three times their damages) in amount to be determined
2 at trial;
- 3 D. Award actual, compensatory, statutory, and consequential damages;
- 4 E. Award equitable monetary relief, including restitution and disgorgement of all ill-gotten
5 gains, and the imposition of a constructive trust upon, or otherwise restricting the
6 proceeds of Defendant's ill-gotten gains, to ensure an effective remedy;
- 7 F. Award pre-judgment and post-judgment interest at the highest rate allowed by law;
- 8 G. Award Plaintiffs and the Classes their costs of suit, including reasonable attorneys' fees
9 as provided by law; and
- 10 H. Award such further and additional relief as the case may require and the Court may deem
11 just and proper under the circumstances.

JURY DEMAND

12
13 Plaintiffs demand a trial by jury on all claims so triable as a matter of right.
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FILED UNDER SEAL

1 Dated: February 28, 2022

2 Respectfully submitted,

SCOTT + SCOTT ATTORNEYS AT LAW LLP**BATHAE DUNNE LLP**

3 /s/ Kristen M. Anderson

4 /s/ Yavar Bathaee

5 Kristen M. Anderson (CA 246108)

6 Yavar Bathaee (CA 282388)

7 kanderson@scott-scott.com

8 yavar@bathaeedunne.com

9 The Helmsley Building

Edward M. Grauman (*pro hac vice*)

230 Park Avenue, 17th Floor

egrauman@bathaeedunne.com

New York, NY 10169

Andrew C. Wolinsky

Tel.: (212) 223-6444

awolinsky@bathaeedunne.com

Fax: (212) 223-6334

445 Park Avenue, 9th Floor

New York, NY 10022

Tel.: (332) 322-8835

Christopher M. Burke (CA 214799)

cburke@scott-scott.com

David H. Goldberger (CA 225869)

dgoldberger@scott-scott.com

Kate Lv (CA 302704)

klv@scott-scott.com

Hal D. Cunningham (CA 243048)

hcunningham@scott-scott.com

Daniel J. Brockwell (CA 335983)

dbrockwell@scott-scott.com

600 W. Broadway, Suite 3300

San Diego, CA 92101

Tel.: (619) 233-4565

Fax: (619) 233-0508

Brian J. Dunne (CA 275689)

bdunne@bathaeedunne.com

633 West Fifth Street, 26th Floor

Los Angeles, CA 90071

Tel.: (213) 462-2772

LEVIN SEDRAN & BERMAN LLP

Keith J. Verrier (*pro hac vice*)

Austin B. Cohen (*pro hac vice*)

510 Walnut Street, Suite 500

Philadelphia, PA 19106-3997

Tel.: (215) 592-1500

Fax: (215) 592-4663

kverrier@lfsblaw.com

acohen@lfsblaw.com

Patrick J. McGahan (*pro hac vice*)

pmcgahan@scott-scott.com

Michael P. Srodoski (*pro hac vice*)

msrodoski@scott-scott.com

156 South Main Street, P.O. Box 192

Colchester, CT 06415

Tel.: (860) 537-5537

Fax: (860) 537-4432

AHDOOT & WOLFSON, PC

Tina Wolfson (CA 174806)

Robert Ahdoot (CA 172098)

Theodore W. Maya (CA 223242)

Henry J. Kelson (*pro hac vice*)

2600 West Olive Avenue, Suite 500

Burbank, CA 91505

Telephone: (310) 474-9111

Facsimile: (310) 474-8585

twolfson@ahdootwolfson.com

rahdoot@ahdootwolfson.com

tmaya@ahdootwolfson.com

*Interim Co-Lead Counsel and Executive Committee
for the Advertiser Class*

FILED UNDER SEAL

ATTESTATION OF YAVAR BATHAE

This document is being filed through the Electronic Case Filing (ECF) system by Yavar Bathae, who attests that he has obtained concurrence in the filing of this document from each of the attorneys identified on the caption page and in the signature block.

Dated: February 28, 2022

/s/ Yavar Bathae
Yavar Bathae